

https://dspace.org/

Applying Blockchain Technology to Improve Higher Education

Yiannakis, Yianna

2025
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/48298
Yiannakis, Yianna . (2025). Applying Blockchain Technology to Improve Higher Education [Master's dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/48298

Downloaded from a DSpace repository. https://dspace.org/



Applying Blockchain Technology to Improve Higher Education

Masters Thesis

2023-2024

by Yianna Yiannakis

Supervised by Andre Gopal

Abstract

This thesis identifies the transformative potential of blockchain technology that can be utilised in enhancing the quality and integrity of higher education processes, with a specific focus in the South African context. The research primarily concentrates on two aspects: first, the detection and prevention of fraudulent admission practices, particularly the use of counterfeit NSCs (National Senior Certificates), and the verification of degrees and diplomas issued by higher educational institutions, thereby ensuring their credibility. Secondly, to investigate the possibilities of blockchain being used to provide a decentralised educational database, accessible to students across the nation, potentially revolutionising how academic information is used, stored, shared, and protected against piracy. Given the innovative nature of the recommendations, a balanced analysis of the advantages and drawbacks related to the implementation and ongoing maintenance of such technology is presented. The research in this thesis is wholly of a theoretical, critical, and argumentative nature, and will not use coursework to validate its components, aiming to contribute to an exponentially evolving discourse on the nexus of blockchain technology and education reform.

Plagiarism Declaration Page

University of the Witwatersrand, Johannesburg

School of Arts
Humanities
Wits Digital Arts

SENATE PLAGIARISM POLICY

Declaration by Students

I, Yianna Yiannakis (Student number: 2090024), am a student registered for MA Digital Arts in the year 2025. I hereby declare the following:

● I am aware that plagiarism (the use of someone else's work without their permission and/or without acknowledging the original source) is wrong.

● I confirm that ALL the work submitted for assessment for the above course is my own unaided work except where I have explicitly indicated otherwise.

● I have followed the required conventions in referencing the thoughts and ideas of others.

● I understand that the University of the Witwatersrand may take disciplinary action against me if there is a belief that this is not my own unaided work or that I have failed to acknowledge the source of the ideas or words in my writing.

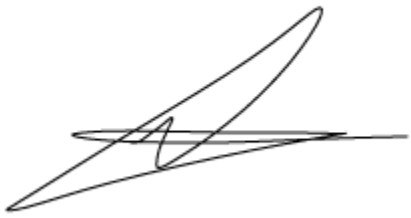
Signature:  Date: 2025-03-28

Table of Contents

Abstract 1
Table of Contents 3
List of Figures and Tables 5
Chapter 1: Introduction: 6
1.1 Research Topic 6
1.2 Research Question 7
1.3 Aim: 7
1.3.1. Security and Validity 8
Figure 1 9
1.3.2. Educational Resources 9
Figure 2 10
1.4 Problem Area 11
1.5 Structure 15
1.6 Limitations 16
Chapter 2: Literature Review 18
2.1. Introduction 18
2.1.1 The Proposition of Blockchain in Educational Institutions 19
2.1.2 The Research Gap within South Africa 20
2.1.3 Implementation of Blockchain within South Africa 22
2.1.4 Understudied Phenomena 23
Table 1 24
Table 1: Fundamental Key Definitions 24
2.2 Security and Validity 25
Figure 3 26
2.2.1 Methods of Online Authentication 26
Figure 4 27
Figure 5 29
Figure 6 30
Figure 7 31
Figure 8 32
Figure 9 42
2.2.2 Centralised vs Decentralised Database 43
2.2.3 Recognising Current Methods of Counterfeiting 49
2.2.5 Socio-Economic Causes of Digital Counterfeiting 51
2.3 Educational Resources 53
2.3.1 Examples of Existing Blockchain Databases 54
2.3.2 Current States of Existing Blockchain Databases: Are they successful? Useful? 56
Chapter 3: Methodology 57

3.1 Introduction....57
3.2 Choice....57
3.3 Framework....58
3.3.1 Saunder et al.'s Research Onion....59
Figure 10....59
3.4 Strategy and Approach....59
3.5 Philosophy....60
3.6 Data Collection Procedures....61
3.7 Limitations, Validity and Reliability....63
Chapter 4: Results & Literature Analysis....65
4.1. Results....65
4.1.1 Research Question 1....65
Finding 1.1....65
4.1.2 Research Question 2....66
Finding 2.1....66
Finding 2.2....66
Table 2....67
4.2 Literature Analysis....82
4.2.1 Research Question 1....82
Table 3....87
4.2.2 Research Question 2....98
Conclusion....104
References....108

List of Figures and Tables

Figures

Figure 1: A summarized outline of the aims within security and validity.....**9**
Figure 2: As summarized outline of the aims within educational resources.....**10**
Figure 3: An infographic showing the framework for the section of the Literature Review.....**26**
Figure 4: An infographic showing the two main methods of online authentication.....**27**
Figure 5: Example of the process of Symmetric Key.....**29**
Figure 6: Example of the process of Asymmetric Key.....**30**
Figure 7: Example of an asymmetric key in the form of a business model.....**31**
Figure 8: Example of an asymmetric key in the form of a cryptocurrency/NFT model.....**32**
Figure 9: Example of a watermarked image.....**42**
Figure 10: The Saunder's et al.'s Research "Onion" Framework.....**59**

Tables

Table 1: Key Definitions.....**24**
Table 2: Research Findings (Results).....**67**
Table 3: An example of a hash function.....**87**

Keywords: Blockchain, NFT, cryptocurrency, SHA-256, SHA-1, SHA-3, counterfeit, steganography, hash functions, hashing, digital signatures, digital certificates, cryptography, artificial intelligence, PIN, ciphertext, plaintext, PKI, DLT, encryption, decryption, spycraft, RSA, MDA, ECDSA, secp256k1, decentralized, centralized, pedagogy, smart contract, quantum computing, eLearning, Blockcerts, Internet of Things (IOT).

Chapter 1: Introduction:

This chapter provides the reader with background information on the study as well as an indication of its intended purpose. This chapter opens with a comprehensive description and contextual background of the research topic, continued with identifying problems areas. This leads to the declaration of the research questions that the thesis will address, followed by an indication of the thesis' structure and limitations.

1.1 Research Topic

Blockchain technology is the foundation on which digital cryptocurrency and **N**on-**F**ungible **T**okens (**NFTS**) have exploded in popularity and financial success. Blockchain is defined **simply** as a transparent database, aiming to collect accurate information for public use. The concept of blockchain technology is that it is an **umbrella** for a large host of different uses and applications, as seen in the birth and financial success of NFTs and cryptocurrency. In 2023, there are still controversial opinions on the subject matter due to a lack of existent government legislation, unethical business practices, and significant security breaches. This was the consequence of simply not having enough time for safety regulations to match the rapid proliferation of new technological innovations and products. It was only in October 2022 that the Financial Sector Conduct Authority (FSCA) in South Africa, declared that cryptocurrency and NFTs were legally identified as a **financial product**, as reported in an article “South Africa regulates crypto” by African Law & Business and author Robert Li (2022).

An ongoing effort to implement local government regulation has been put in place to manage the growth and perpetuation of blockchain projects**.** As a result, there is an established and regulated entry into the market, with norms and laws and the potential for consequential arrest if they are not complied with. With this information, it is evident that blockchain volatility is being noticed, addressed, and remedied, bringing confidence to blockchain research as a whole. Blockchain technology in itself has notably been severely overlooked by educational institutions and society,

thus opening an overwhelmingly vast expanse of potential research opportunities in its positive impact on daily life. It would be a shame to disregard the innovative nature of blockchain, which can potentially enhance the quality and integrity in internal operations and functions, particularly focused within the context of South African higher education institutions; specifically universities, colleges, or postsecondary professional schools.

1.2 Research Question

There are two main direct research questions that this thesis aims to answer reads as follows;

1. *How can unique blockchain encryption technology be used to secure and validate higher education institutional product outputs (diplomas, degrees, and certificates) to fight counterfeiting, and what resources would it cost to implement and maintain such technology?*

2. *How can blockchain technology be used to introduce valuable educational resources, such as decentralised, open-sourced data centres; what would their benefits and drawbacks be as opposed to current-day existing resources?*

1.3 Aim:

The overarching aim of this paper is to construct theoretical methods of action for utilising emerging blockchain technologies within the context of higher educational institutions, while critically analysing and measuring how realistic it would be to implement in South Africa. The information measurement is based on current local and international research, including case studies, project initiatives, and related data. The thesis establishes a focus on the **primary characteristics** of blockchain, such as it being immutable, decentralised, unanimous, and utilising primarily **SHA**-256 (**S**ecure **H**ash **A**lgorithms) hash encryption for high-end security. Then knowing said highlighted characteristics, it can be applied to higher educational institutions in the context of various internal functions, in order to collect suggestions on the improvement of functionality and quality of life for both core establishment functions and students. There are two main research areas that are being addressed: first, security and validity in relation to institutional functions, and second, online educational resources that can help students and research.

1.3.1. Security and Validity

Firstly, the core aim of this section is to determine how blockchain technology can secure and validate education product **outputs** to fight counterfeiting within South Africa specifically. This would include degrees, diplomas, certificates, and professional qualifications that a student has achieved within a tertiary educational institution. It would also be beneficial to focus not only on the **output** of higher education qualifications, but also on fraudulent matriculant certificates (*National Senior Certificates*) used to apply for entry **into** courses/degrees.

There is an aim to identify current local case studies, such as the website MiE acquired by EOH Holdings Limited in 2014, which offers paid online public services to validate and authenticate multiple types of legal documents nationwide and continental within 30 African countries (and accessible globally since it is online). This gives evidence that there is an effort in addressing the lack of availability of external, reliable verification services. As this thesis particularly focuses on South Africa, it leads to a legitimate reason for how educational institutions should be a part of this effort - as it is extremely beneficial to fighting counterfeiting. However, the purpose of compiling information on a **comparison** of the benefits and disadvantages of a closed, centralised database (such as MiA) to one that uses blockchain, can provide valuable information. It aims to determine similar trends between the two databases, reveal existing unfulfilled gaps, as well as describe and clarify information for the reader (which is essential for addressing having "*digestible pieces*" of information as a characteristic of this thesis).

The first section branches off into smaller focus groups that link from the previous one. This includes an aim of **recognizing the current methods** used to create virtual counterfeit materials (such as, but not only limited to, online identity theft for certificates) in 2023, allowing an establishment of potential gaps and limits in typically used security technology. Another particular local case study of counterfeit problems is identified again in Ignasio M. Jimu's article (2018), stating that the existence of scanning, copying, and reproduction technology has presented overbearing challenges. Notably, having the inability to track perpetrators accurately and decipher between real and fake qualifications. His paper notably **identifies** the causes of resorting to counterfeiting within developing countries; as well as offering a general, **vague** recommendation on implementing and regulating countermeasures against it. However, there is a severely-lacking amount of detail in providing concrete steps to achieve this goal.

Therefore, it is an aim to thoroughly investigate blockchain technology, to measure its **uses** and **potential expansion**, particularly looking into international and local case studies that are **already** utilising this through existing research and developing technologies. Then, apply found information to South African universities while being mindful of the implementation and ongoing maintenance of such technology.

Figure 1

The following highlights the main active steps and proposed variables in this section:

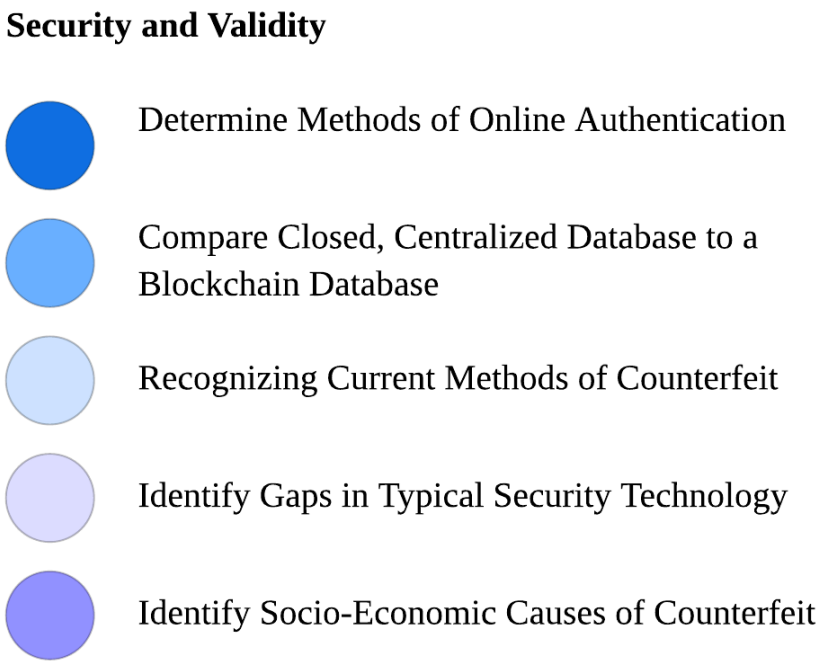


Figure 1: *A summarized outline of the aims within security and validity.*

1.3.2. Educational Resources

Universities could benefit from looking into decentralized databases which use blockchain technology to collect credible, **transparent** information locally for educational purposes, as seen on websites such as *Hedera*, which hosts applications for a vast array of valuable and educational

databases. Utilizing SHA-256 hash encryption, these databases provide authentication and enforced security, preventing third-party users from tampering with information.

Because one of the aims of this thesis is to determine outside possibilities rather than what is commonly considered to exist, this concept is applied to current, regular educational databases and how blockchain may manage it differently than how it normally functions. Following the **identification** of these technological advancements, the factors to be estimated are the prospective benefits and drawbacks. Keeping in mind the existence of virtual and physical libraries, what potential risks they currently present, and how blockchain could offer an innovative way of doing research. There is targeted research on current applications that use blockchain technology, specifically using the case study *Hedera* (as mentioned briefly in the above paragraph), to determine micro-database examples and provide potential evidence of success.

Figure 2

The following highlights the main active steps and proposed variables in this section:

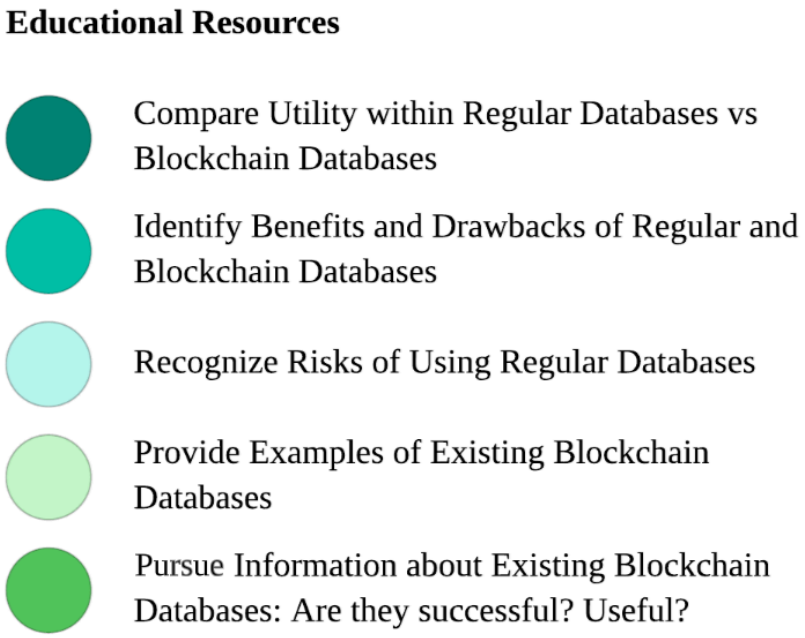


Figure 2: *A summary of the educational resources section's aims.*

1.4 Problem Area

It is critical to note that this paper approaches blockchain by looking at a spectrum of outside possibilities rather than what is popularly believed to exist, such as NFTs or cryptocurrency which are often and popularly associated with the term. There is a noticeable lack of general fundamental understanding of blockchain technology, evidently because it is such a recent and **complicated** concept emerging as a popular topic of interest in 2008 under the pseudonym *Satoshi Nakamoto*, according to Robert Sheldon's (2021) article, "A Timeline and History of Blockchain technology". Thus, this clearly shows there is a great need for research to break down information into metaphoric "*easily digestible pieces*" for an average user that may not have enough time to investigate the *rabbit hole* of definitions independently. Blockchain technology is conceptualized as an umbrella term, often hosting many projects that use parts of this technology to function. It is also a concept based on an old method of book-keeping, a time-stamp being its true core characteristic: A mark of time, according to Mark Mwandosya and Matthew Luhanga's (2020) journal article, "Blockchain: A Disruptive and Transformative Technology of the Fourth Industrial Revolution". Along with understanding the characteristics and functions of blockchain, it will be applied within this thesis to analyse and formulate innovative ideas for South Africa to utilise to improve life for higher educational institutions and their students.

Furthermore, identifying **hacking techniques** and how online **fraud** is produced would be valuable in the aim of recognizing gaps in our current systems. Particularly, but not limited to, virtual techniques such as *steganographic Malware*, *document fraud*, *institutional fraud*, *diploma mills*, *accreditation fraud*, *and translations (p.51)*. It is important to note that this research equates to a droplet of effort compared to the ocean that is intercepting hacking and counterfeit-generation techniques, which **cannot** overcome the threat. Exactly how cutting off the head of the Greek serpent "Hydra " will spawn three more, it is conglomerative, ongoing, and adaptive to its environment, making it so versatile,complicated and hard to handle.

However, with the understanding of potential vulnerabilities, blockchain technology can be implemented with awareness of these threats and potentially provide a realistic and practical system capable of protecting information in South Africa - while being cautious. While it may seem that identifying basic information on the vulnerabilities of local technologies can be subjectively hazardous, establishing information on various hacking and counterfeiting techniques gives the opportunity to determine **boundaries** for blockchain technology according to Nikita Stupin, seen in

CoinDesk's article "OpenZeppelin Reveals Top 10 Blockchain Hacking Techniques in 2022" by Sage D. Young (2023), proving it to be beneficial. As mentioned at the beginning of this paper, there is a current rapid proliferation of new technological innovations, but importantly, the same can be said for the creation of counter-opposition with criminal intent. There are more details on this information in the *Chapter 2: Literature Review* (p. 18) section of this thesis.

Focusing on the aspect of **boundaries**, attention is given to analysing the two types of encryption (symmetric and asymmetric) and hashing within cryptographic algorithms in order to assess their strengths and limitations, as well as how blockchain SHA-256 functions are characterised and utilised compared to the other six SHA algorithms. According to the National Institute of Standards and Technology, The Computer Security Division (2023) describes in their online article "Hash Functions" an overview the seven internationally-approved hash function algorithms; " SHA-1, SHA-224, **SHA-256**, SHA-384, SHA-512, SHA-512/224 and SHA-512/256", as well as SHA-3. The thesis also looks at MDA and SHA-1. Putting effort into identifying detailed information on exactly what blockchain technology uses in its processes can provide existing data on the implementation of blockchain technology within local, institutional processes, and have the **ability to estimate** the workload intensity of implementation, maintenance, and security of possible systems for South African institutions. In addition, determining the uniqueness of SHA-256 amongst its cousins and family group will also give strong background evidence of its utility when compared to current local technologies (in the context of security, validity, and educational resources) used in South African higher education institutions.

Additionally, it would be useful to learn what **motivates** people to engage in counterfeiting and online security breaches, as this would lead to identifying the factors (e.g socio-economic issues) as a contributing element that negatively impacts South African higher educational institutions.. One simple, brief example is the effects of poverty and financial desperation that resort to people applying for jobs with fake qualifications, identified according to Ignasio M. Jimu's article (2018), "Fake Qualifications and the Challenge of regulating Higher Education in Southern Africa". Importantly, however, in the larger context, blockchain is reliant on an internet connection, suggesting that it is vital to be aware that there is always the additional danger of extra **international** threats in addition to local concerns. This section in the paper will be smaller in comparison to the other subtopics, however, it is important to put it in as recognition of the context as a whole.

While this thesis has the disadvantage of not having research conducted through questionnaires or surveys locally, unlike the previously mentioned papers above, it benefits from current information that has already been conducted **internationally** and applying it to the South African context. By choosing this research methodology, information collected can potentially suggest a **higher standard** of data, due to universal frameworks already funded, researched and developed, and exhibit results on the effect of its implementation. Importantly, it gives the ability to analyse what would be suited best for South Africa, as well as deter ideas that may have already had a negative consequence when it was applied in the real world.

It is the core, methodical motivation for conducting this analysis, having the capability to **gauge** the level of technological advancement based on South Africa's current systems and determine what is currently holding South Africa back from implementing effective technological changes. This includes identifying current systems, their vulnerabilities and how blockchain technology may have the ability to resolve these issues. When these elements of this research are identified, **only then can quantitative investigations be introduced and conducted** if there are particular glaring problem areas.

Additionally, the entirety of this thesis and research provides a unique perspective since it records **South Africa's** technological status in 2024 and documents its transition into the 4th industrial revolution, offering **evidence-based theories** on how to integrate innovative system models in the qualitative nature of the thesis's methodology. It would be useful for the current age and the specific region, and also simultaneously provide a historical record if this paper is read in the far future. This research is more impactful than existing international studies as it is contextualized into a **developing country**, offering inspiration in the development of solutions upon identified outdated forms of technologies - the focus being the efficiencies of databases, prevention of online fraud and counterfeit when entering into the digital era. The thesis is also designed to **challenge** current frameworks that exist in South Africa, specifically focused on higher education institutions, and offering a detailed guideline and forward extension into innovative and progressive technology.

Furthermore, this research is nonlinear and expansive, since it may branch out into the contexts of government and public amenities and services, such as e-commerce, healthcare and government services. This branching out is justified as the thesis finds that to answer the core research questions in the context of higher educational institutions, it is important to scope amenity aspects within South Africa, **situating** the research in its region and reiterating the extent of the research

gap. An example is expanded on in the *Literature Review*: *The Research Gap within South Africa* (p. 20-21) due to the discussion of similar efforts made within South Africa, which involves a case study describing and detailing the development and implementation of time-saving, efficient and technological progressive e-governance within South Africa in 2024. Though the point is that the research can be applied in a broader context, it is important to reiterate that the thesis **always** has education in its best interest - concentrated on the South African setting and higher education institutions. As a result, the thesis offers a unique perspective in that it focuses not just on the research questions, but also on **how** the research interacts with the surrounding environment.

Lastly, the research is also unique as the information presented is desired to be comprehensive to readers who are **not** familiar with extensive mathematical concepts nor high technological dialect, inducing a larger scope of reachability and understanding of an inevitable digital progression of history and time. In validation of this, Johnathan Bevers's (2021) thesis, available online as open-source academic material, "The Study of Symmetric and Asymmetric Key Encryptions" had also reiterated and reaffirmed the same point in their own research. The evidence and further discussion is provided in *Chapter 4: Literature Analysis, Research Question 1* (p. 80), where in summary, there is a lack of research papers that accommodate simplicity in the writing.

As a researcher offering my own perspective on this, the thesis is primarily designed to contribute academically to a broader scope of simple readability, allowing readers to understand and adapt to technological advancements and human progression as a whole. To not express curiosity in a possibly **helpful** and **innovative** solution to current-day frameworks would indicate dormancy. Focusing on the context, the role of blockchain technology in higher education may simultaneously advance South Africa in various ways, however, also bring awareness to the **risk of stagnation** in our current technology as well as **offer solutions** to already-existing problems.

For instance, if certificates could only be validated using blockchain technology on the website of the online institution from which they originated, the possibility of counterfeit certificates could be **completely eliminated**.

With the development of adaptive artificial intelligence and its ease of access and functionality by the user, it poses a risk to stagnating countries with a lack of digital framework or foundation in their educational institutions. This includes the potential use within counterfeit and fraud of official certificates, a loss of preservation of unique historical and academic data and intellectual output,

and the loss of opportunity to utilize blockchain-based databases that may offer an advantageously enormous amount of democratized (and potentially [1]cross-disciplinary, collaborative) data.

Thus, this research is significant in establishing the first steps of applying and weighing the potential of the blockchain technology concept specifically within the context of South African higher educational institutions. In academic contribution, as a thesis, it can add to scholarly research and literature within the field of innovation technologies, as well as determine the current state of technology and formulate general methods of improvement within university or institution practices.

1.5 Structure

The structure of the thesis is as follows;

Chapter 1: The Introduction presents the research topic explicitly, a brief contextualization as well as the supporting research sub-questions. This chapter also includes the overall purpose, why it is important and presents a proposed outcome.

Chapter 2: Literature Review is the bulk of the thesis, as it is the most important section. The chapter is divided into three sections. The chapters will be organised according to the core *Research Questions* (p. 7) outlined in *Chapter 1.*

The first section will be the Introduction, which focuses on the Proposition of Blockchain in Educational Institutions, identifying the substantial Research Gap within South Africa, the Implementation of Blockchain within South Africa, and finally covering the concept of Understudied Phenomena.

The second section will be focusing on the first core research question in the context of Security and Validity. This includes sub-headings covering Methods of Online Authentication of Legal Documents, Centralised vs Decentralised Databases, Recognising Current Methods of Counterfeiting, Gaps in Typical Security Technology, and finally Socio-economic Causes of Counterfeiting.

The third section will be focusing on the second core research question in the context of Educational Resources. This includes sub-headings covering Utility between Regular Databases and

[1] *According to Dictionary.com*, it is the overlap of two or more different academic disciplines and fields of study with a comparable link, such as an example of natural and geographical sciences.

Blockchain Databases, Benefits and Drawbacks between Regular Databases and Blockchain Databases, Risks of Using Regular Databases, Examples of Existing Blockchain Databases, and finally Current States of Existing Blockchain Databases, analysing if they are successful or useful.

Chapter 3: The Methodology will present the appropriate, qualitative approaches to the study, as well as explain justification of why these approaches were chosen. Simultaneously, when these are presented, the reader will gain a further understanding of the limitations of the chosen study approaches.

Chapter 4: This chapter will be used to discuss, review and analyse the multitude of qualitative data collected from the previous chapters, searching for common themes, main findings and gaps to apply and conclude the main thesis research questions, and supporting research sub-questions.

1.6 Limitations

The research methods used in this thesis have distinct limitations that should be acknowledged. It is dealt with in the following way;

Firstly, due to the research topic focusing on a relatively newer concept of technology, it is dependent on whatever primary source information is available. An example of this is determining the results of newly implemented blockchain technology into universities, an example being the recent conceptualised and implemented student achievement validation database and introduction of digital currency as a kind of student credit. *This is discussed further in Literature Review: The Proposition of Blockchain in Educational Institutions* (p. 19). Their results are still ongoing and yet to be determined a success or a failure.

Secondly, multiple case studies were chosen as the research source due to their ability to discover and highlight present shortcomings. This also gives the ability to focus purely on the two core research questions. There is a vast amount of information that is available to dissect into the context of the research questions. With this understanding, publication bias can be avoided as multiple sources of information will be looked at, avoiding indulgence within specific and minimal case studies. However, sorting through so many different sources of information is far more time consuming.

Thirdly, this thesis adopts a **qualitative, argumentative** research style, with the fundamental goal of scaling the best solution to presented questions using existing **researched data** and **theory**, as well as real-world **reactions** from similar circumstances internationally. While it is useful to present the best, logical theory, according to Joseph A. Maxwell's (2023) book, "Qualitative Research Design: An Interactive Approach", it is also advantageous to identify *understudied phenomena* surrounding research. What might look good on paper might have had a different outcome in real life.

There is an expectation that while these innovative suggestions are not expected to be definitive, it is an acknowledgement and direction of a plausibly progressive future of the state of South African quality of education.

Chapter 2: Literature Review

2.1. Introduction

In Guang Chen, Bing Xu, Manli Lu & Nian-Shing Chen's (2018) article, "Exploring blockchain technology and its potential applications for education", they emphasise their conclusion that there has been relatively insufficient blockchain research and that **studying themes on future educational revolutions would be difficult**. The challenge would be that it was so **new**, and blockchain technology was being implemented with no information on the outcomes. It is understandable that it would have been a daunting time to implement such technology; as it would be like jumping into unknown waters.

Advancing to the next year, the article "Blockchain-Based Applications in Education: A Systematic Review" by Alammary et al. (2019) focuses on identifying multiple research papers that have been published, and studies that have been conducted, in the context of implementing blockchain technology into educational institution systems. This article also includes multiple infographics that show the number of papers found for each core research topic addressed in the study, easily indicating the most prominently occurring topic to their reader. A great substantial total of **2321** articles that mention blockchain technology within educational institutions were identified and extracted in benefit to their original, core research questions, such as one that identifies similar ideas within "Benefits that Blockchain could bring to Education" (Alammary et al., 2019). It gives an accurate reflection of the present state of blockchain technology worldwide, as it outlines the core ideas that are commonly presented and **repeated** in a vast amount of recent research papers. It also suggests that there is a growing interest in investigating the potential of blockchain technology, however it is still premature and within theoretical speculation. Importantly, however, this information is extremely useful to **this** thesis as the qualitative and analytical nature of the article shows the concept of *understudied phenomena*, as previously and briefly mentioned in the *Chapter 1: Introduction* (p. 5) section of this paper. While it is practical to determine logical theory with the most likely predicted outcomes, the complexion of this article by Alammary et al. provides an outside perspective on how other academics may unpredictably evaluate and finally categorise informational material as least and most favourable.

2.1.1 The Proposition of Blockchain in Educational Institutions

Additionally, in the research article "Blockchain technology and education" by Grigore Albeanu (2017), they go into specific detail describing that blockchain technology is engineered in such a way that guarantees transaction irreversibility (inability to undo an action), prevention of counterfeiting and double spending. Circling back to the particular article mentioned in 1.1 above by Guang Chen, Bing Xu, Manli Lu & Nian-Shing Chen's (2018), there is a proposition of how educational institutions can reform their systems to have blockchain technology enhance the *online learning experience* such as the idea of a student achievement validation database, implementation of digital currency as a form of student credit (to be able to earn and use it around campus), as well as the concept of a smart contract which regulates the quality of work output (Chen et al., 2018). Being aware that this article was posted in 2018, there is a timeline from then until 2023 where we can determine how much research has been conducted since. It is also clear that this particular article has established groundwork and given validity to the potential of using blockchain technology within educational institutions, as these proposition suggestions relate directly to the core research questions within **this** thesis. It also suggests **multiple** ideas for how blockchain technology may be used, providing evidence for why it is worth researching.

Furthermore, **this** thesis is also **unique** in that most research papers situate themselves in theoretical-analysis contexts, and do **not** go into intrinsic detail on how exactly blockchain technology may remedy security gaps. In an example, there is an investigation in **this** thesis on general cryptography, steganography, how blockchain encryption technology (hash functions or 'hashing') is created and functions, and can possibly be effective in enhancing systematic processes within South Africa. This includes determining exclusive characteristics of SHA-256 hash in comparison to other hash encryptions, which was further explained in the *Rationale* part of this paper. Strikingly, it also establishes the present state of blockchain technology as of 2023, taking into account ongoing and implemented research and providing a platform for examining real-world applications. Consider *Maryville University* in St. Louis, Missouri, United States, which was one of the first educational institutions to install a blockchain database in 2019.

Having a university that has previously implemented a blockchain ledger within their premises validates the purpose of **this** thesis, which questions *why South Africa cannot do the same.* Furthermore, the research conducted in **this** thesis may suggest which keys and functions could be implemented into a university. It may provide detailed information on the purpose and offer

guidance on how blockchain technology might be used to improve and integrate university operations for applicants, students, faculty, administrators, and the general public.

2.1.2 The Research Gap within South Africa

Linking back to the first few paragraphs of this *Literature Review*, these two research papers mentioned there that have been conducted and written **internationally** - from Saudi Arabia and Taiwan specifically. After conducting a search through multiple sources, the findings suggest that there is **no** specific information or research relating to the context of South African **educational institutions.** Although, a similar research paper to the context of this thesis would be "Antecedents of the adoption of blockchain to enhance patients' health information management in South Africa" by Dineo A. Matlebjane and Patrick Ndayizigamiye (2022), which emphasises the impactfully **positive** potential of blockchain technology being applied to healthcare system operations and data management within the South African context. Included in the research is a qualitative investigation study conducted in the form of interviews, focusing on collecting data for both Information Technology (**IT**) and healthcare professionals to determine difficulties and frustrations from both their perspectives within current local technological systems. Crucially, some of the participants of this study suggested that healthcare information needs to be standardised, and the South African eHealth strategies first needed to be prioritised and implemented before proposing a further enhancement in introducing blockchain technology (Matlebjane & Ndayizigamiye, 2022).

Highlighted in Guangyuan Chen's (2024) research article, "Optimizing Digital Signatures for Enhanced Privacy Protection in Blockchain Systems", they explain that blockchain technology may be advantageous and greatly prevent unauthorised access to extremely sensitive patient medical records. Through access control and encryption, blockchain may also easily enable the exchange of medical data between various healthcare organisations while protecting patient privacy. This technology can bleed broadly into supply chain management, healthcare, governance as well as **educational institutions**.

In further research conducted now in **local** context to assess the current actions taken to address this above issue, The South African eHealth strategy, according to the National Department of Health (2012) in their journal, "National Digital Health Strategy for South Africa, 2019 - 2024", seeks to develop and provide a national, digital platform for storing healthcare data on patients, medicine, and human resources. According to the World Health Organization's (**WHO**) webpage (2019),

“National Digital Health Strategy for South Africa 2019-2024”, the nine strategic interventions had stated that the implementation of the digital health platform is to be completed by 2024. The latest news report, found in an article online by BizCommunity (2024), “#BizTrends: NHI to boost South Africa's digital healthcare”, states that it is still in progress and is closer to completion. As of the 27th of February, the time this article was published and at this point of the thesis, there have been no further reports.

However, what is interesting to note is while conducting research on the South African eHealth Strategy, interest was piqued on a news article written and posted online on Cape Town Today’s webpage (2024), “South Africa’s Digital Transformation: A Leader in E-Government Development” by Isabella Schmidt. The article highlights the creation of The National e-Government Portal, an initiative within South Africa to **progress** and **improve** government services by digitising physical lineups (including Home Affairs), reducing turnaround times, and increasing efficiency. Ultimately, a digital infrastructure that is progressively moving forward into the 4th Industrial Revolution, as the article mentions South African e-governance developed in conjunction with the *Data and Cloud Strategy* and the *National AI Plan.*

A practical example and evidence that South Africa is moving forward into the 4th Industrial Revolution can be found at https://www.ekurhuleni.gov.za/, where government services are clearly accessible via a public, digitised platform; it is appropriate for the public because a citizen and/or entrepreneurs gain access to services, information, forms (that may be filled out digitally and submitted online), as well as all official information and communication released by the government.

This information makes it evident that South Africa has made an attempt to acknowledge its technological deficit, address its concurrent problems, and catch up to global standards. Therefore, the **core research questions in the thesis can be situated within ongoing and diverse initiatives,** indicating the research’s **usefulness beyond the core context of the thesis** (usefulness within higher education institutions). It also identifies the regions of the nation that are leading and falling behind, evidently suggesting that e-governance (electronic-governance) and e-healthcare (electronic-healthcare) strategies have been put in place, which means e-education (electronic-education) **should** follow shortly. Therefore, the thesis seeks to propose, analyse and discuss a framework in an attempt to prompt and encourage meaningful progression within South Africa.

2.1.3 Implementation of Blockchain within South Africa

While it is clear to say that healthcare and governance in South Africa is **not** a focus of **this** main thesis, it poses the vital questions of whether **educational institutions** have a priority framework previously established and the ability to possibly implement technological systems such as blockchain technology. Furthermore, having this information demonstrates a gap in research and evidence of why it is **essential** to research and identify the national roadblocks to technological advancement, whether they are (previously mentioned) poverty or socioeconomic difficulties within South Africa that may need to be solved first before adopting this notion. It also emphasises the **importance** of determining whether blockchain technology has the potential to possibly help to alleviate the country's identified current issues, thus it validates one of the core research questions in this paper. **In summary**, it presents an unsolved question if current higher educational institutions have an established framework to be able to implement innovative technological enhancements.

To put it simply, does South Africa have existing foundations to build and expand on?

As an existing trend, another similar journal article, "A principal component analysis of barriers to the implementation of blockchain technology in the South African built environment", published by Akinradewo et al. (2022), identifies **the general boundaries** that South Africa has to implement such technology and provides the results of a snowballing sampling data collection technique. According to their findings, implementing blockchain technology into routine operations would create unique problems, such as technological obstacles and the need to reiterate their original systems (which is time consuming and costly). Possessing such information aids in showing that this research was conducted to evaluate whether it is realistically feasible to execute within a society that already has operational frameworks. This also includes the expense of maintaining such technology in terms of not only funds but also an adequate staff. This information can be extremely useful in appreciation of **this** thesis, and shows evidence that researchers are considering such implementation, as well as provide data on helping answer the questions posed in the previous paragraph.

2.1.4 Understudied Phenomena

What is also important to point out is that this same journal article above references Steven Leibson's (2018) online article "Blockchain is not Bitcoin—Bitcoin is not Blockchain" which stipulates the misunderstanding of blockchain being defined with direct association to Bitcoin and NFTs. As previously mentioned in the first sentences of the *Chapter 1: Introduction* (p. 6) of this paper, blockchain is the umbrella that provides the foundation for an array of uses and applications. Bitcoin and NFTs are only **a product** of this technology. This online article emphasises the significance of how new academic research and writings on innovative technologies must be conscious of *understudied phenomena* (unexpected results from theoretical ideas) and provide an educational introduction and clarity to such themes. With this knowledge, it is evidence to why this thesis aspires to possess the quality of having "*digestible pieces of information*," as previously described in this paper's *Aim* section.

Ironically, after reappraising the *Literature Review*, *understudied phenomena* are far more glaringly prevalent than expected.

Holistically looking at the two previously mentioned papers in the subheadings above, by Dineo A. Matlebjane and Patrick Ndayizigamiye (2022) and Akinradewo et al. (2022), they both clearly demonstrate a continuing effort in South Africa to investigate blockchain technology, **initiate** and **survey** information within the context of South Africa, and justify this thesis by showing the prominent research **gap** that it intends to fill. Additionally, it is also clear that these studies indicate that most of them are using quantitative methods of research in the form of sampling techniques, surveys and questionnaires in an effort to recognise and bridge a chasm within online informational sources.

While it is important to also discuss and compare literature reviews of other author's research articles and papers, this thesis will follow a certain methodology. First, **core definitions** will be indicated and explored in the context of the sub-heading relating to the core research questions. 'Exploration', in this case, would be to provide a comprehensive and contextual understanding - defining the terms that are newly presented to the thesis and thoroughly understanding their historical background, purpose and application to the context of the paper. This gives an opportunity for the thesis to provide discussion in *Chapter 4: Results & Literature Analysis* (p. 63) section, and open prospects to identify *Understudied Phenomena* and introduce formulated concepts based on given evidence. After reading through the *Literature Review*, it is clear that a subtle

deductive research methodology has been used. In order to provide a thorough grasp of the underlying theory and enable **accurate** discussion and application of theory to core research questions, it first presents a broad research topic before gradually deflating and breaking it down into the inner workings of blockchain technology.

Table 1

Table 1: Fundamental Key Definitions	
1. Cryptography	Hides the message (Krzyzanowski, 2024).
2. Steganography	Hides the **existence** of the message (Krzyzanowski, 2024).
3. Spycraft	A *noun*, the skills, technology, tools and techniques used by spies, YourDictionary (2024). The aim of spycraft is to keep, hide or steal secret and valuable information. Spycraft and Tradecraft are the same thing.
4. Encryption	The process of which digital information that has been changed into **secret code**.
5. Decryption	The process of **secret code** that has been changed into digital information.
6. Ciphertext	The **secret code**. Cannot be read until it is decrypted.
7. Plaintext	The digital information that is readable to a human. Also when the **secret code** is decrypted.
8. Symmetric Key	The same key that is used for both encrypting and decrypting information (Thales, 2024).
9. Asymmetric Key	One key is used to encrypt information, and another key is used for decrypting the information (Thales, 2024).
10. Digital Signature	A mathematical algorithm that generates a unique digital fingerprint. (Chen, 2024).
11. **P**ublic **K**ey **I**nfrastructure **(PKI)**	A set system (foundation) with specific rules to control public/private key mechanisms (Qurotul Aini et al., 2022).
12. **D**istributed **L**edger **T**echnology **(DLT)**	Two-party facilitation without a trusted, mutual third party (Mwandosya and Luhanga, 2021).
13. Hash Functions/	A *noun*, a digital security tool that encrypts data into a fixed

Hashing	output value, despite the length of the input value YourDictionary (2024). It is a robust digital security tool.

***Table 1**: The above table contains simple, condensed, brief key definitions for the terminology used throughout this section of the thesis. This is also a useful reference point to return to, and contextualises definitions.*

2.2 Security and Validity

How can unique blockchain encryption technology be used to secure and validate higher education institutional product outputs to fight counterfeiting, and what resources would it cost to implement and maintain such technology?

As mentioned in *Chapter 1: Introduction* (p. 6), the subsection is structured as follows; it will be focusing on the first core research question (as seen in the above paragraph) in the context of Security and Validity. This includes sub-headings covering Methods of Online Authentication, Centralised vs Decentralised Databases, Recognising Current Methods of Counterfeiting, Gaps in Typical Security Technology, and finally Socio-economic Causes of Counterfeiting.

The purpose of Methods of Online Authentication is to identify the most widely used algorithms and **security** techniques while also providing a chance to find any gaps that raise discussion about the potential applications of blockchain technology. It also seeks to provide thorough background information in the form of outlining definitions and giving explanation to the core concepts found.

This presented knowledge conveniently **bleeds** over and into the Centralised vs. Decentralised Databases where the information gathered is appropriately applied to the thesis research question in the form of a comparative analysis. Recognising Current Methods of Counterfeiting, Gaps in Typical Security Technology and Socio-economic Causes of Counterfeiting is focused in applying research within the context of South Africa and higher education institutions. In *Figure* 3, the infographic below, it indicates what was discussed now and presents a useful, clear view of how this section of the Literature Review is structured.

Figure 3

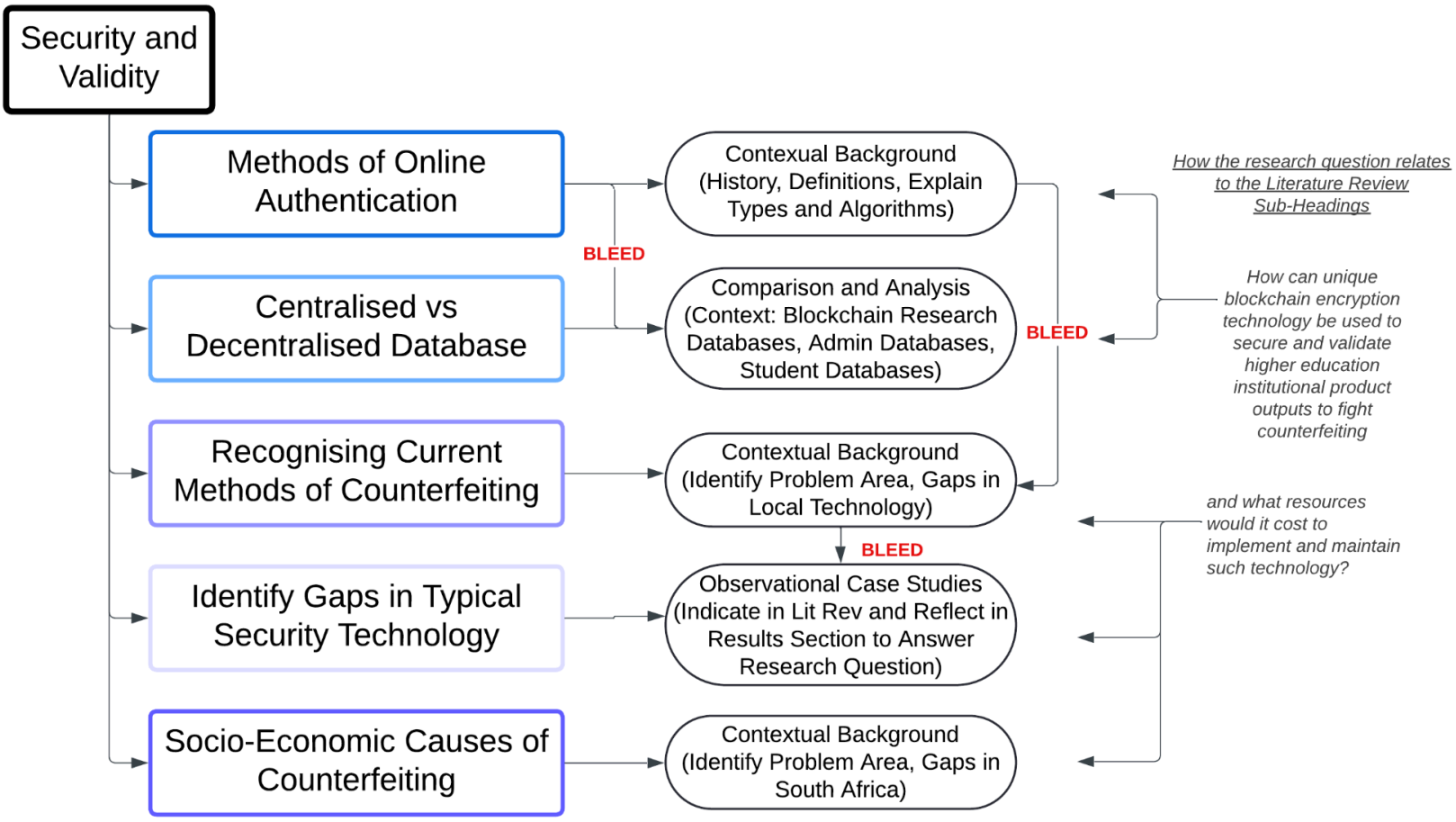


Figure 3: *A detailed infographic showing the framework for this section of the Literature Review, the purpose, expectation of information and how it assists in answering the core research question.*

2.2.1 Methods of Online Authentication

While the thesis aims to explore blockchain technology, it is extremely beneficial to discuss other solutions and algorithms, and eventually compare on how blockchain would challenge these. In doing this, it offers a **competitive** and unbiased conclusion, providing the most practical theoretical solutions after considering internal and external contexts.

In researching methods of online authentication and providing a foundation for further literature

analysis later in the paper, Mathe, R, et al.'s (2012) journal article, "Securing Information: Cryptography and Steganography", introduce two primary kinds of digital authentication techniques:

Cryptography and **Steganography.**

In *Figure* 4, the infographic below, it introduces the two main methods of online authentication for digital security, along with its respective sub-categories. Since **hash functions** and **digital signatures** are a component of cryptography, they were not particularly covered in the aforementioned publication; yet, because of their potential for critical analysis later on in the paper, they merit appropriate attention in this thesis. This information structure has been simplified and streamlined to highlight the major points that the thesis seeks to address.

***Figure* 4**

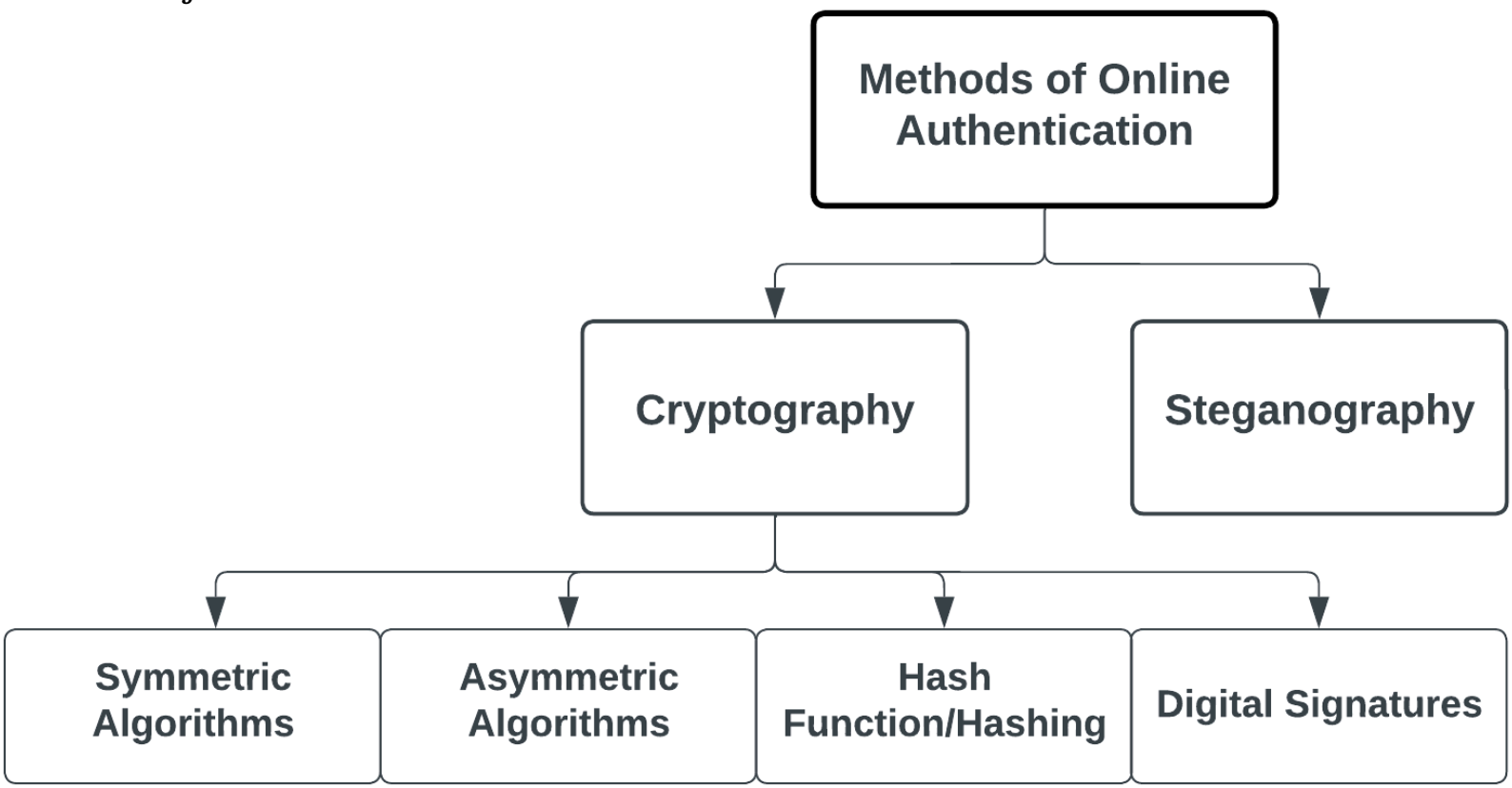


***Figure* 4:** *An infographic showing the two main methods of online authentication, as well as the relationship hierarchy of the sub-categories.*

Cryptography

In Mathe et al.'s above-mentioned journal article, "Securing Information: Cryptography and Steganography", they provide modern-day context for both the terms *Steganography* and *Cryptography*. **Cryptography**, in a brief definition, are the broad mathematical techniques used in "*security science, ensuring privacy, integrity of data, entity authentication, and data origin authentication*" (Mathe, R, et al., 2012). According to Paul Krzyzanowski's (2024) online article, "Steganography & Watermarking", the simple purpose of cryptography is that the contents of a message is **concealed** - as opposed to steganography where the message is **completely hidden** to an unknowing viewer. The user would be unaware that there was a message in the file in the first place.

Cryptography is split up in Symmetric, Asymmetric Algorithms, Hash Function/Hashing and Encryption. The academic definition, explanation, brief historical context and practical examples are as follows:

Symmetric (Private) Algorithms

To put it in a simple example in the context of the 21st century, getting a parcel from a trusted courier is an instance of barebones symmetric cryptography. The courier asks for a secret number (the 'key' or **PIN** (**P**ersonal **I**dentification **N**umber)), and once provided by the receiver, the interaction is authorised and the parcel is handed over. **Both** participants know what the secret key is. What was just described is an example of a **Symmetric key.** Both encryption and decryption is done using a singular key, and is often referred to as a *secret key*, as it is kept in a *secure channel*, as clearly described in Alenezi et al's (2020) journal article, "Symmetric Encryption Algorithms: Review and Evaluation study". Again, placing this in the context of the simple courier example, the secure channel would be communication between the courier and the receiver via **SMS** (Short Message Service).

Below is *Figure* 5, an infographic on the Symmetric (Private) Key and its process of encrypting and decrypting information. Both keys are used to *encrypt* and *decrypt* ciphertext. Ciphertext, to an outsider, is incoherent and impossible to understand. In simple summary, *Figure* 5 it shows **three algorithms**, as explained in Jonathan Katz and Yehuda Lindell's (2007) book, "Introduction to Modern Cryptography: Principles and Protocols", the key-generation (1), the encryption (2) and the decryption (3). This book is particularly useful when understanding the intricacies using algebraic

equations and may be a great academic resource recommendation to further the study outside of this thesis, however, it is **not** necessary to relay it here right now.

***Figure* 5**

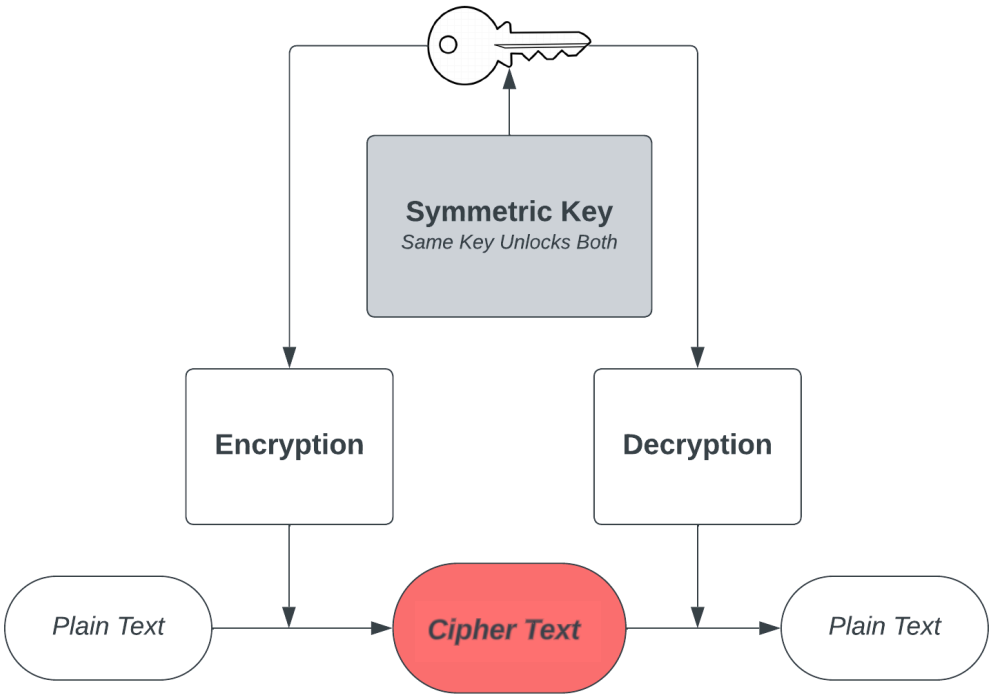


***Figure* 5:** *Example of the process of Symmetric Key.*

Asymmetric (Public) Algorithms

According to Johnathan Bevers's (2021) thesis, available online as open-source academic material, "The Study of Symmetric and Asymmetric Key Encryptions", they explain complicated asymmetric algorithms comprehensively and simply, and that asymmetric keys solve the issues that symmetric keys have. Asymmetric Keys are used when there needs to be **additional security** onto documents. There are two keys, "*one to lock or encrypt the plaintext and another to unlock or decrypt the ciphertext. Neither key performs both functions*" (Bevers, 2021). One key is secret and one key is public. **Encryption** is used with the **public key**. The ciphertext is decrypted using the **secret key**. The reason why this algorithm is referred to as a 'public key', is that the public key is shared

amongst others, however, the **owner** keeps encryptions secure with their private key. In *Figure 6* below, this shows an example of a barebones process of an asymmetric key.

Figure 6

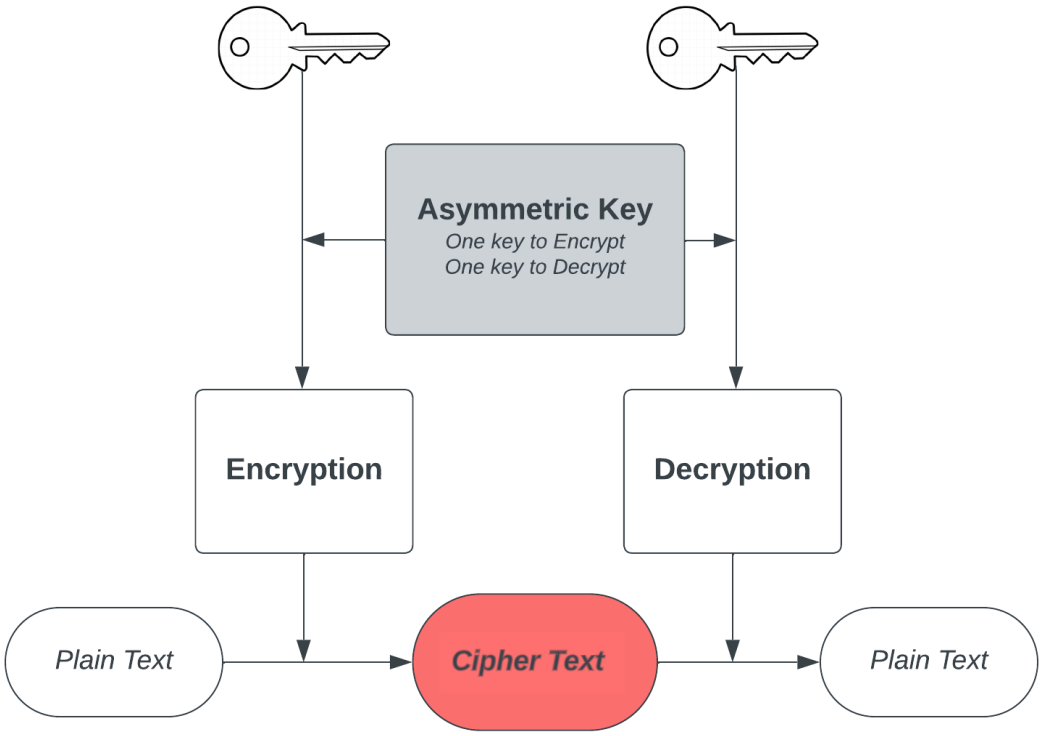


Figure 6: *Example of the process of Asymmetric Key.*

The public key is used to encrypt, and the owner keeps and ensures the security of the encryption with their private key. **Their private key** is **completely different** from the public key. If this was put into a real life example of an operation within a business, the operations would look like *Figure* 6 below. Below Figure 7, *Figure* 8 shows how an asymmetric key functions in the transactions of cryptocurrencies in the context of trading NFTs.

***Figure* 7**

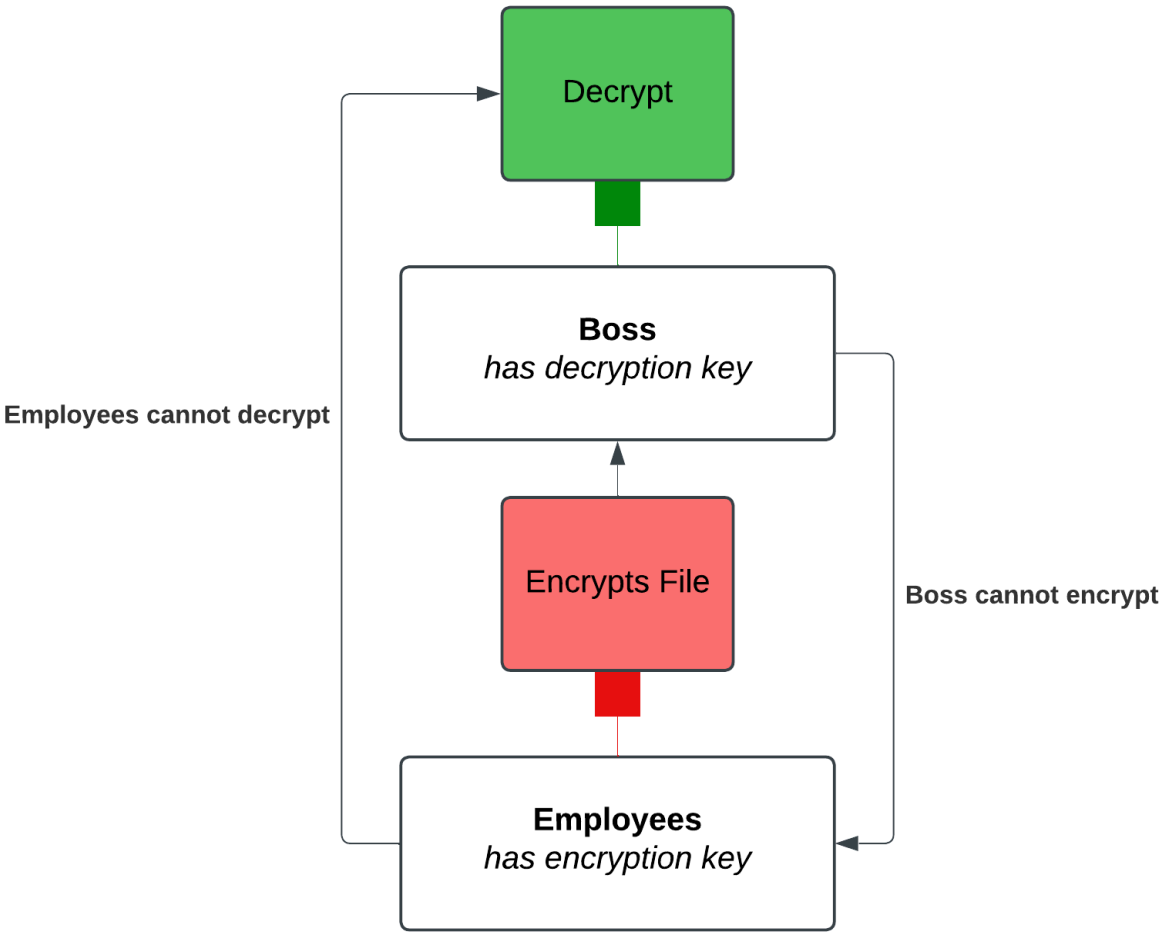


Figure 7: *An example of an asymmetric key in the form of a business model within a corporate institution.*

Figure 8

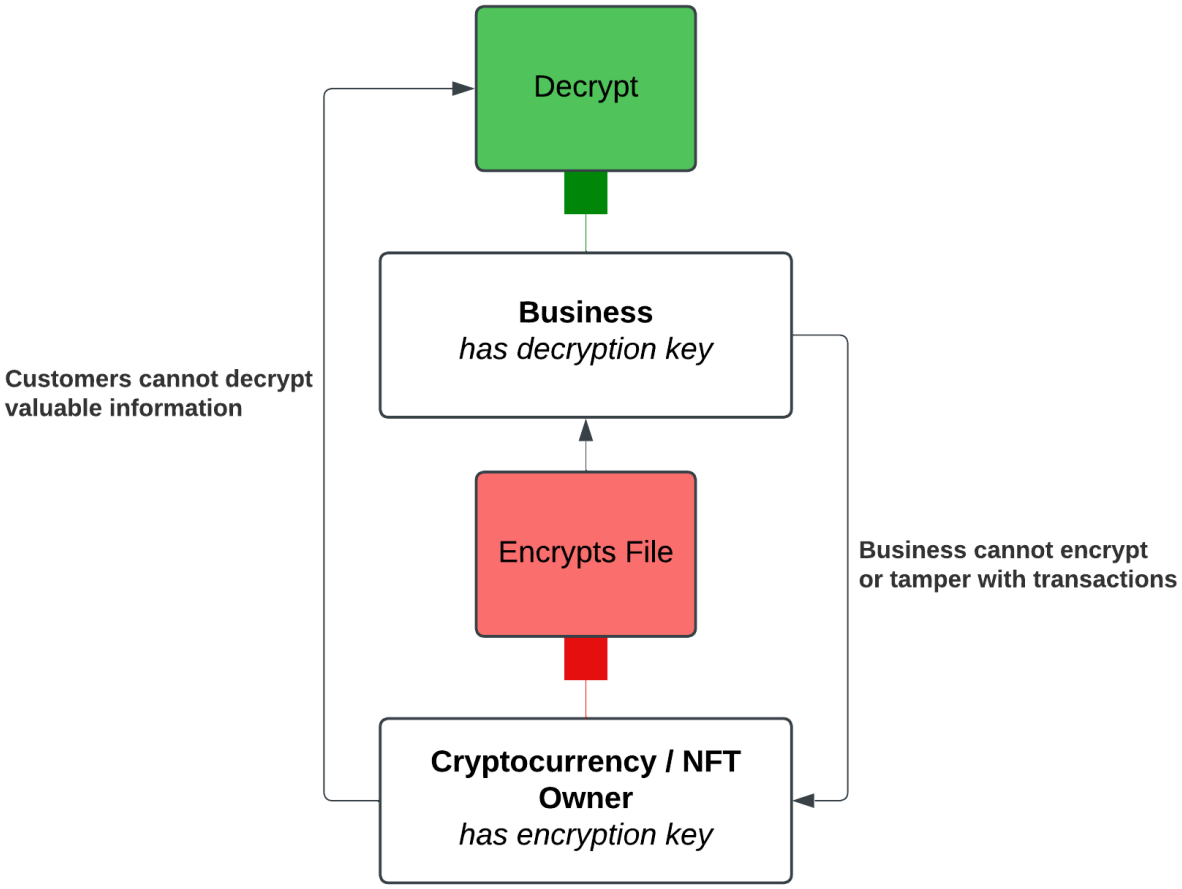


Figure 8: *An example of an asymmetric key in the form of a cryptocurrency/NFT model.*

Hash Functions/Hashing

Bleeding from symmetric and asymmetric algorithms above and into this section of the thesis, hash functions are intertwined with the research; as this section describes how encryption **works theoretically**, how to **encrypt practically** and its **overall functionality**. To apply and respond to the core research questions appropriately and contextually, it is critical to present and understand **foundational theory**, which can then be elaborated upon later in the thesis in the form of pragmatic **critical analysis**. The purpose of this section is to fulfil a necessary, logical requirement of presenting the various approaches and strategies used in hash functions/hashing, as well as elaborating on the functionality of current blockchain technology, projecting its evolution from

SHA-2 into SHA-3, and analysing its suitability for use in South African higher education institutions.

In Rajeev Sobti and Geetha Ganesan's (2012) journal article, "Cryptographic Hash Functions: A Review", they discuss and build upon referenced Praveen Gauravaram's (2003) thesis, "Cryptographic Hash Functions: Cryptanalysis, Design and Applications", thus importantly pointing out and noting the year difference between both academic texts, as well as the time of this thesis is written (2024). This indicates **evidence** that hash functions or 'hashing' have existed for a considerable amount of time. Conclusively, it has proven to be a vital tool to assist with digital security, due to the longevity of its existence and practicality seen with the successful **symbiotic** use within blockchain (cryptocurrencies popular examples include *Ethereum*, *Binance Coin* or *Dogecoin*).

The general key characteristics of cryptographic hash functions or 'hashing', both described by Rajeev Sobti and Geetha Ganesan's (2012) journal article and in Qing Zhou et al.'s (2023) research article, "Quantum-inspired Hash Function Based on Parity-dependent Quantum Walks with Memory (August 2023)", is that this is a **mathematical algorithm** that offers a solution to ensure "*digital identification, message authentication, digital signatures and pseudorandom number generation*" within a modern society and its available and expanding digitized services (Qing Zhou et al., 2023).

Sungbeen Kim and Dohoon Kim's (2024) research article, "Data-Tracking in Blockchain Utilizing Hash Chain: A Study of Structured and Adaptive Process", explains functionality of hash functions or 'hashing', expecting the mathematical algorithm to **always** output a fixed-size value regardless of input length. An example to simplify this concept is if meat is then grinded into mince. If you just had the mince, the mince (the output) cannot be determined or converted back into its original form. The output of a fixed-size value (*the mince*) is commonly called the hash value (GeeksforGeeks, 2022). The encrypted output (it is **encrypted** because the input length has been **converted** to a fixed-size value) is then recorded onto a fixed hash chain, which is immutable and prevents any tampering. A live example (and demonstration) of a website that generates hashing from strings can be accessed through this following link: SHA512/256 - Online Tools.

Importantly, according to Shashwat Sharma and Ayush Mishra's (2024) research article , "A Comprehensive Study of Cryptographic Hash Functions", they further explain that if there is **one**

minor change to the input variable, it will drastically change the output variable (hash value). In brief summary, this information indicates that the process is **trustless**, immutable, automatic and secure, as there is therefore no central authority; and in support of this statement, the same point has also been mentioned in Marut Pandya's (2024) research article, "Performance Evaluation of Hashing Algorithms on Commodity Hardware".

Another characteristic of hash functions or 'hashing', conveniently brought up through Qing Zhou et al. 's (2023) research article, is in their research and discussion of mainly developing a quantum-based hash function - interestingly using, in their words, "*theoretically* ***infinite possibilities*** *of the initial state and the irreversibility of modulo operation*". It is important to mention this briefly, as it is necessary evidence to explain that there are a **variety of hash functions** developed according to a variety of distinctive needs.

Therefore, referring back to the earlier sections, it is evident that hash functions, or "hashing," can have either private or public encryption because, as was previously mentioned, hash functions are **not** all the same. Noting a particular point from Sungbeen Kim and Dohoon Kim's research article, which primarily focuses on data-tracking and intentionally threat-testing these algorithms (exposing any potential weaknesses or collisions), they included a comment which commended hash algorithms for their ability to be **extremely sustainable in a "*resource-constrained environment*"** that demands quick data processing and validity verification (Kim and Kim, 2024).

This is where the mention of **SHA-256** becomes relevant. In GeeksforGeek's (2022) online website article, "Blockchain Hash Function", they describe a few classes of hash functions including **R**ACE **I**ntegrity **P**rimitives **E**valuation **M**essage **D**igest (**RIPEMD**), **M**essage-**D**igest **A**lgorithm (**MDA**), BLAKE2, Whirlpool and **Secure Hashing Algorithm**. According to Shashwat Sharma and Ayush Mishra's (2024) research paper, SHA-256 particularly is primarily used in blockchain technology due to the balances between performance and security in comparison to other hash functions. Each block on the blockchain contains a hash of the previous block, forming an impossibly adjustable chain. In the research article's recommendation, MD5 and SHA-1 are still used in older models, but are obviously more susceptible to collision attacks and grow **obsolete** as time and digitization progresses. Applications that need more sophisticated cryptographic strength and data with exceptionally high security may consider using SHA-3, the most recent iteration of SHA, which could eventually replace SHA-2 as the industry standard.

Digital Signatures, Digital Certificate and Encryption

Digital Signature

The research articles mentioned below is purposely thorough, as a general observation, it is evident that there are many research papers that **broadly** outline the advantages and disadvantages of using blockchain technology in various contexts. This includes higher education institutions, as there aren't any that provide a **clear** path forward, offer a **deeper** understanding of how digital signatures might work within a system, or explain how one would go about selecting or developing a system. This is also because technology is always changing and programs are subject to change. *Chapter* 4: *Results & Literature Analysis* (p. 63) goes into additional detail on this topic, specifically in *Literature Analysis*: 4.2.1 *Research Question* 1 (p. 80).

A digital signature, according to Guangyuan Chen's (2024) research article, "Optimizing Digital Signatures for Enhanced Privacy Protection in Blockchain Systems", is (typically) a private key using a cryptographic mathematical algorithm to generate a **unique digital fingerprint** for the purpose of ensuring authentication, integrity and prevention of repudiation - imitating the concept of a real-life stamped fingerprint, as it is basic knowledge that an exact fingerprint on human fingertips is genetically impossible. Like the discussion of hash functions in the subsection above, is it clear that **cryptography is an essential tool that offers many methods to a fixed solution**, therefore similarly indicating that the creation of a digital fingerprint using cryptographic techniques offers the same amount of choice (depending on the needs of the system).

In Guangyuan Chen's (2024) research article above, they also importantly introduce three of **multiple cryptographic algorithms** primarily used for creating digital signatures; **RSA** (**R**ivest–**S**hamir–**A**dleman), **DSA** (**D**igital **S**ignature **A**lgorithm) and **ECDSA** (**E**lliptic **C**urve **D**igital **S**ignatures).

Simply explained in the research article, "A Secure Multiple Elliptic Curves Digital Signature Algorithm for Blockchain" by Wei Bi, Xiaoyun Jia and Maolin Zheng (2018), digital signatures both **symbiotically** use public key cryptography and hash functions. Bitcoin, for example, uses the elliptic curves digital signature algorithm (ECDSA) to authenticate transactions, additionally renowned in its **30% increased algorithmic speed and efficiency** in comparison to other curves. As an example, the specific name for the epileptic curve that Bitcoin uses is **secp256k1**.

Interestingly, this research article above proposes **multiple** elliptic curve digital signature algorithms (with the addition of MECDSA) and ultimately suggests a security enhancement by implementing **two** elliptic curves due its difficulty of solving ECDSA. This demonstrates the astounding rate at which technology is developing, which provides evidence that there is a desperate need to match aggressively progressive digitization upgrades, further discussed in *Literature Analysis*: 4.2.1 *Research Question* 1 (p. 80).

Critically, in Guruprakash Jayabalasamy and Srinivas Koppu's (2022) research article, "An empirical study to demonstrate that EdDSA can be used as a performance improvement alternative to ECDSA in Blockchain and IoT", one of the research questions they review is how **various** elliptic curve cryptography can be used in blockchain technology to protect patient privacy in medical records and administration. This can easily be applied into the context of higher education institutions. Focusing back to the article, they indicate the historical slow technological transition of the digital signature from **RSA** to **DSA** to **ECC** (Elliptic Curve Cryptography). The successor of ECC is an **EdDSA (**Edwards Curve Digital Signature Algorithm) that shows, through testing, its robust performance, quick arithmetic, and resistance to hash collisions. However, a final point the article highlights is that **EdDSA** and **ECDSA** usage is **case-dependent**.

In emerging ***understudied phenomena***, according to Deepanshu Rana's (2024) journal article, "Advancements and Comparative Analysis of Digital Signature Algorithms: A Review", they bring up the point of **standardization** in an example of the efforts of the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI), whereas there is an attempt at frameworking a chosen 'post-quantum cryptographic algorithm' that meets certain criteria for certain protocol. This brings up the discussion of the same concept applied within the thesis question (particularly in *Literature Review*: 2.3.1 *Implementation of Blockchain within South Africa* (p. 22)), the same idea that was brought up within this thesis earlier in regards to setting a framework and standardization within South Africa. However, in the article above, it said that institutions would need to engage in collaborative teamwork efforts for this to happen. *Literature Analysis*: 4.2.1 *Research Question* 1 (p. 80) discusses this further in the consideration of standardization discourse.

However, the journal article identifies the major threat of **quantum computing** in the near future, a rapidly-emerging technology scientifically defined (within *Dictionary.com's* (2025) online website definition) as an extremely powerful vessel that may simultaneously act on multiple pieces of data

within one singular operation. In comparison, a common computer will only act on one piece of data at a time. It is only a matter of time until new algorithms are implemented which hold such technology, posing a threat to former algorithms as the computing power will be just enough to deem many as obsolete. Therefore, in Deepanshu Rana's (2024) journal article above, they indicate that in the future, ***"post-quantum cryptography algorithms can offer security in the face of quantum computers".*** A promising feature mentioned was the use of blockchain technology as a useful foundation that may offer a secure and authentic digital signature solution to rapidly progressive and aggressive technologies - therefore, indicating that blockchain will prevent potential problems in the future if it is implemented **now**. Additionally, they suggest practical real-world applications, such as organisations that have to identify their security needs before implementing blockchain technology.

Therefore, there are many options for hash functions, algorithms, digital signatures and methods of cryptographic security options, making it glaringly obvious that **there is not a linear way of implementing blockchain technology**. A Master's thesis would not be able to be addressed as thoroughly as desired due to the limited capacity and scope, however, this gives potential for further research and intends to contribute to research. This is further discussed in *Literature Analysis: 4.2.1 Research Question 1* (p. 80).

Digital Certificate

According to Shuyi Pu and Jasmine Siu Lee Lam's (2023) research article, "The benefits of blockchain for digital certificates: A multiple case study analysis", they describe digital certificates as the evolved successor of physical certificates (documentation). This can be in an example of a **PDF** file (**P**ortable **D**ocument **F**ormat). With the outbreak of COVID-19, a digital certificate was needed to prevent physical contact. However, with the emergence of blockchain technology, digital certificates may incorporate blockchain characteristics of its security; validity, security, authenticity and reliability.

They discuss a case study called "***BlockCerts***", which attends to and prevents credential forgery within education institutions, using the main characteristics of blockchain technology (as previously mentioned in the previous paragraph). A main point discussed within the research article was the merging of physical certificates into digital certificates, however, in the education context, there is a clear opportunity that digital credentials may be issued. As a result, using

blockchain technology incorporated into digital certificates, it resulted in "***BlockCerts"*** helping with better human resource management as it employs a legitimate workforce, saving time for staff as they may utilize that for more "***value added services***" (Pu and Lam, 2023). This applies to both the university as well as potential employers for when students graduate and leave school.

In an additional sub-point, Pu and Lam also indicate that there is a lack of deeper insight on how beneficial blockchain digital certificates may be, adding another author as evidence to agree with the thesis's statement that there **needs to be more understandable, foundational research and spread of awareness.**

Encryption

According to Jean-Philippe Aumasson's (2024) book, "Serious Cryptography, 2nd Edition: A Practical Introduction to Modern Encryption", they indicate that encryption and digital signatures are used in conjunction with each other, aiming to ensure **confidentiality** and enhance security. Encryption is basically scrambling data, enough so that it becomes intelligible and into a secret code. It may only be unlocked via a digital key. Asymmetric and Symmetric Keys are forms of Encryption.

Therefore, in Guangyuan Chen's (2024) research article investigation into ECDSA, it was additionally conducted to address privacy problems and improve digital environments, as blockchain digital transactions are characteristically transparent. Chen (2024) proposes a solution to address this, such as **zero-knowledge proofs** and **homomorphic encryption**.

According to Liz George and Jubilant Kizhakkethottam's (2021) research article, "A Comparative Study of Zero Knowledge Proof and Homomorphic Encryption in Guaranteeing Data Privacy in Blockchain Applications", they indicate the evolution of blockchain technology implemented into sectors outside of cryptocurrency, such as the example of smart contracts within the supply chain that demands privacy and confidentiality (George and Kizhakkethottam, 2021). Both the previous two research articles discuss zero-knowledge proofs and homomorphic encryption to be the **most major** solutions to this problem. Simply, zero-knowledge proof is providing evidence of the transaction, however not leaking sensitive information. Homomorphic encryption, explained from its Greek meaning of '*same structure*', the data being able to be worked with in its ciphertext **without it being decrypted**. Only the private key-holder will be able to decrypt the information

and understand it. A simple example would be if people voted for something of significant importance online, the data will be able to retain privacy through its handling, computing the results only for the accessibility of the private-key owner (George and Kizhakkethottam, 2021).

Blockchain

Therefore, using the aforementioned concepts and specific descriptions, Blockchain may be defined contextually within the reader's understanding. According to Mohammad Usman's research article, "Understanding Cryptocurrency, Blockchain and the Market", they simply state that Blockchain is a database that keeps information differently from a typical one; ***data is saved in blocks that are linked together, whereas standard databases store data in tables***. When new data is received, it creates a new block that is chained to the previous block. They are ordered chronologically, keeping integrity of the transaction and the time it was uploaded. The chain of blocks is stored on nodes that autonomously cross-check each other 24/7, which can be in various locations - eliminating a single point of weakness. Therefore, applying this mathematically, according to Christopher King's (2022) journal article, "Some mathematical topics in blockchain and digital ledger technology", using one-way **ECSDA** to generate digital signatures to prove authenticity. "***An elliptic curve is the locus of points satisfying an equation of the form y2 = x3 + ax + b"*** (King, 2022). More specifics on the mathematical aspects of **ECSDA** may be found in their research article. However, in the conclusion of their study, **inversion** of this operation within **ECSDA** is impossible without brute force or random trial and error due to the use of modular division as a result of multiplication arithmetic of the curves. Hashing (**SHA-256**) is the creation of a digital fingerprint, an authorization of the unique user transaction within the node. Thus, when working in tandem with each other, the user generates data into their hash using **SHA-256**. The hash is then signed by the user with a private key with **ECSDA,** and outsiders may check with the public key and authenticate the signature was from the real person.

If this is put into the context of using it within an education system, students will have their private key and their credentials hashed (as if they are putting their digital fingerprint on them). **ECSDA** will then come in to verify the user. An outsider may have the public key and be able to rely on **ECSDA** to authenticate the user and the credentials.

Steganography

Steganography is an important part of online authentication, as it is seen to accompany cryptography to strengthen security and authenticity. As Mathe, R. and et al. state, interestingly, both terms (Steganography and Cryptography) are original cousins of **spycraft** (Mathe et al., 2012). YourDictionary (2024) defines **spycraft** as a *noun* to describe "*the skills, technology, tools and techniques used by spies*". As Foreign Policy says in their online article, written by Edward Lucas, "Changes in technology, politics, and business are all transforming espionage. Intelligence agencies must adapt—or risk irrelevance",

> ***"A cover identity that would have been almost bulletproof only 20 years ago can now be unravelled in a few minutes"*** (Lucas, 2019).

According to the article "An Innovative Approach of Verification Mechanism for both Electronic and Printed Documents" by Haque et al. (2020), they further identify multiple methods of digital document protection. These include "*digital watermarking*, ***steganography***, *digital signatures and blockchain*".

The term **'steganography'** has been offered an additional abundance of information, revealing that there are multiple forms of protecting *(or hiding)* digital data as a whole. In order to simplify this term, it can be understood as a progressive art of cryptic science throughout history - the concepts of invisible ink and morse code messages were in effort to conceal the transit of messages until the receiver has access to it (Haque et al., 2020). According to Margie Semilof and Casey Clark (2023) in Tech Target's website "steganography", the definition of **steganography** is aimed at hiding data in various complex ways. It is similar to cryptography as both are engineered to secure data; however, what distinguishes steganography from the latter is that it conceals the fact that the file has been encrypted with hidden messages. Data is encrypted into files such as JPEG images, audio or video files. When done correctly, files will look no different to the original (Semilof & Clark, 2023).

In Luca Caviglione and Wojciech Mazurczyk's (2022) research article "Never Mind the Malware, Here's the Stegomalware", they give a good example to validate the above literature; Malware is a **broad definition**, (narrowed down to viruses, worms, trojun viruses, spyware, adware, ransomeware

and rootkit, sniffers, keyloggers and spam, as stated by Rabia Tahir's (2018) article "A Study on Malware and Malware Detection Techniques"), with the common characteristic being that it is malicious and intends to harm the computer and/or the user. It has been harder to detect due to its combination and mutation with steganographic techniques (hiding malicious code within innocent-looking files). In an additional point to support and give evidence to what was said earlier in this thesis, in *Introduction*: 1.4 *Problem Area* (p. 11), as digital science progresses, so does the criminal.

However, after researching steganography with the above case studies, the definition of steganography commonly results in it characteristically being **ambiguous and varies in degrees of visibility**. While encrypting data in an image is used to carry hidden information, the contrary can be done to fulfil its purpose of guaranteeing a message is readable. In an example, In *Figure* 3 below, it showcases a watermarked image. A watermarked image is a type of steganography in which the original publisher protects the image to ensure that it is not stolen, according to Marie Look's (2011) online article, "How to Add a Watermark to Photos". They also discuss watermarking in the traditional sense, which is when documents are held up to the light to assess whether they are authentic or not. The best example to help support this fact contextually in South African higher education institutions is the case of **diplomas or certificates** that can be held up to the light to declare its authenticity, as well as shining UV lights to reveal an additional layer of authenticity.

Figure 9



Figure 9: *An example of a watermarked image (on the left) compared to a normal image (right).*
Image reference: MDV EDWARDS / SHUTTERSTOCK (2023)

Steganography, particularly watermarking, is emphasised as a crucial topic of interest since, in response to the research sub-question and thesis context, there is evidence of watermarking in the context of a physical degree or certificate earned by a graduate student. Degrees, diplomas or certificates in its physical form have some kind of unique identification: an example being golden stickers, signatures from the institution and holographic imprints. Authentic degrees obtained from authentic sources may include some type of genuine, physical identifier. However, there is a lack of commonality within educational institutions: a genuine **digital** identifier, indicating that there is a significant gap. Digital identifiers, in 2024, are more of a novelty than the norm. The information provided above is applicable to the thesis as it is useful to determine and discuss in the *Literature Analysis: 4.2.1 Research Question 1* (p. 80) on what are the options for higher educational institutions, their older forms of online authentication and how it can be improved, combined or where there are

gaps between the technology and physicality, and discussion of bridging the gap to progress into the 4th Industrial Revolution.

2.2.2 Centralised vs Decentralised Database

Bleeding from the above topics in the previous section, there is a clear understanding and explanation of cryptography, asymmetric and symmetric algorithms, steganography, hash functions, digital signatures, and encryption. With this understanding, it will apply the aforesaid research into the **practical application** of blockchain technology, such as databases used by higher education institutions. The literature will concentrate on research conducted to evince and encourage critical **analysis** of utility (transparency, automation, ease of access, situation of failure, immutability), and security risk (sabotage and hacking risks, third party alteration and privacy). This research provides critical **foundational** work for the thesis's *Chapter 4: Results & Literature Analysis* (p. 63) section.

Therefore, after conducting online research through many open sourced databases such as Google Scholar, ResearchGate and Science Direct, there is evidently a research gap, making it difficult to find specific academic information on both centralised and distributed databases. There are only a few papers that determine their characteristics. Luckily, there have been an increase of academic papers that address **blockchain** as a progressively popular topic of information, which the authors are prompted to include necessary details on centralised and decentralised databases in order to contextualise core characteristics. It is crucial to explore these features because they will provide insight into how security and education are understood and carefully managed inside the context of a higher education institution.

Extremely similar to this sub-research question, the research article previously mentioned in the *Literature Review: 2.1.1 The Proposition of Blockchain in Educational Institutions* (p. 18) section of this paper, "Blockchain technology and education" by Grigore Albeanu (2017) directly compares the commonly used 'Distributed Ledger Technology (DLT)' and 'Blockchain Technology (BLT)' in the context of the core research question of **this** paper, *Applying Blockchain Technology to Improve Higher Education*. This particular article is quite similar to this thesis, and recognises the potential use of hash functions and a decentralised database in education, indicating that there is already **existing** external research on this and **completely** situating, and validating the argument and theoretical proposition of this thesis. The paper dives into general research, identifying that using blockchain technology will be useful for student records, ***new pedagogy*** (*improvement of teaching*

practices- defined by Dictionary.com), smart contracts and student rewards and the introduction of a ***meta-university***. These are multiple, innovative resources that a higher education institution may be able to utilize and enhance the quality of life of their students, staff, health of academic integrity and administrative tasks.

One of the main points that was introduced at the beginning of this paper was that blockchain technology is an **umbrella** for a large host of different uses and applications, but is commonly known and seen in the birth and financial success of NFTs and cryptocurrency. The below quote from the article discussed above validates the point of this thesis: what else can blockchain do for us other than operate within cryptocurrency and NFTs?

"*BTC is more than Bitcoin...*" (Albeanu, 2017).

Centralised Database

According to Abubakar Mohammed and Bashir Maina Saleh's (2017) journal article, "Centralised Database: A Prerequisite for Security and Sustainable Development in Nigeria", a centralised database is a **singular** digital storage database within an organisation. The data/records is collected and stored to allow for the authority of the organisation to **harmonise** information, share, analyse and continuously update the database (Mohammed & Saleh, 2017). Within the bounds of a centralised database, it is accessed through a central point. The database provides for authority customisation, delegating management to a dedicated administrative team, and providing access to specific information for the user base.

This information is validated through a case study, a journal article by Aghayev et al. 's (2008), "Virtopsy – The concept of a centralised database in forensic medicine for analysis and comparison of radiological and autopsy data". This particular journal article expresses the need for a centralised database to address the difficulties of validation and analysis of data within their respective medical field, opting for a **standardised, digital documentation tool**, that may reap the benefits of having an established framework of information that has the flexibility for the data to be shared, analysed and continuously updated (Aghayev et al., 2008). Particularly, one of the benefits they were mostly interested in was the ability to have international collaborations to provide important "***support for forensic-radiological casework and research***". Having collaborative research allows for a higher

quality of research data, additionally contributing to cross-validation, as well as enabling information that broadens the perspective of the potential researcher that is outside of the **demographics** the original research was conducted in. However, the researcher has indicated that there is a concern for sustainability and scalability of the database as the amount of users grows.

A centralised database was introduced to **digitise** physical databases composed of written records. The thesis generally focuses on recently published research articles (2019 and upwards, ideally), but older articles may also be useful in providing historical context, comparing information, and discussing changes in digital databases and blockchain technology. “Centralized versus Decentralized Computing: Organizational Considerations and Management Options”, an old research article, by John Leslie King (1983), explain that centralised databases originated from the idea that employees may ‘telecommute’ and work from home, and is an **evolution** from small-scale departments into networked distributed systems.

It is remarkable to witness and realise through this journal article how centralised versus decentralised databases were debated in the 1980s, compared to the twenty-first century, when it may be argued that the COVID-19 pandemic **reinforced** and drove most firms to rely on and quickly construct a reliable work-from-home system for the sake of economic continuation and survival. This point will be discussed further in *Literature Analysis: 4.2.2 Research Question 2* (p. 96).

Focusing on the security and validity context of this sub-question, this poses the curiosity of the technical aspects of centralised databases. One specific concern raised by the journal article above, by Aghayev et al. (2008), was the sharing of private information in a centralised, standardised database that would be accessible over the internet. It is extremely worth noting that the data should respect laws and ensure that the information includes a certain amount of anonymity within the limitations of ethical information management. It is also very **case dependent**, such as the example of medical research uploaded into a database - it is expected that real medical cases abide by consent and ethical practices of both the participant and the research institution. This applies to **all** research handling human participants. Despite the **notable bias** and **comment posed** by the above authors in regards to the ‘delinquency’ of many things within forensic medical institutions, the authors do make a valid point when discussing the withholding of valuable research from the public. Institutions may feel uncomfortable with sharing valuable (or privatised) information as an open resource. Contextually, institutions that profit from withholding academic research and selling it to readers for their access may "**gatekeep**" potential research that could be utilised and strengthened

globally. This particular point, therefore, sparks a critical discussion of discourse within research findings in the *Literature Analysis: 4.2.2 Research Question 2* (p. 96).

However, according to Joseph Enoch and Bourdillon Omijeh's (2023) research article, "Comparative Analysis of Blockchain and Database", in regards to their statistical findings, researchers may only use approximately half of the true capabilities of modern technologies to tackle a problem. Therefore, applying this **counterpoint** to the research article above, the grandeur of modern technology removes the bounds of a physical library, transcending the scope into an international and unlimited digitized online library - offering the opportunity to also uncover a higher quality of research. Despite this point, the two above articles do share a commonality. Simultaneously, Enoch and Omijeh (2023) indicate that a wealth of information **adds** to the amount of inappropriate misuse of technology. This point of misuse bleeds into the concept of a centralized database, commonly used in business sectors of the economy.

In its most simplistic summary, centralized databases were found to be extremely prone to failure due to the fact that they rely on a standalone, single network. A harmonized network that is customizable, and able to delegate management to a dedicated administrative team (Mohammed & Saleh, 2017) is also **prone** to a **lack of regulation** and **misuse of technology**, either by employees, users or institutions.

Decentralized Database

In brief historic mention, according to Mark Mwandosya and Matthew Luhanga's (2021) research article, "Blockchain: A Disruptive and Transformative Technology of the Fourth Industrial Revolution", they introduce the **origin** of blockchain - indicating that it had used a ledger and time stamping as **an old book-keeping method** to address issues of forgery, double spending and ownership. Fast forward to 2025, according to Julian Springer and Philipp Haindl's (2024) research article, "'Blockchain-based PKI within a Corporate Organization: Advantages and Challenges", **D**istributed **L**edger **T**echnologies (**DLT**) emerged as one of its **digitized successors**, having blockchain as an **option** to incorporate and implement one. They indicate that blockchain technology has been widely used due to its maturity, strong security features and an enhanced compatibility with **P**ublic **K**ey **I**nfrastructure (**PKI**). They, importantly, specify that despite which **DLT** is used, all rely on these specific techniques; secure identities within an insecure environment, multiple points of failure within a scaled peer-to-peer environment, and lack of central authority.

In simple further explanation, decentralized databases maintain a copy of their ledger on a network of multiple nodes, according to Bhabendu Mohanta et al's (2019) review article, "Blockchain technology: A survey on applications and security privacy Challenges". Therefore, as Enoch and Omijeh (2023) research article **supports** and **builds** upon this fact, with a decentralized database, it operates in a way that there are **multiple points of failure**. If the system fails, data may easily be backed up through recovery on another point of entry. Therefore, it is impossible for a **complete shutdown** of a ledger (Enoch and Omijeh, 2023). Apart from a centralized database, blockchain-decentralized databases **do not** require third party management due to cryptographic algorithms automating set processes and functions, which is basically the buzzword "***smart contracts***" that is mentioned multiple times throughout the thesis. A decentralized is far more transparent, due to privacy being in the form of **personal addresses** (with the use of hashing algorithms like **SHA**), and therefore does not show important sensitive information. Blockchain-decentralized databases are therefore **trustworthy** due to the fact that each "transaction" follows rules according to its core engineering and input algorithms.

Interesting, according to Enoch and Omijeh's (2023) research article, one of their findings conclude into an observation that multiple analysis of other similar research articles show **a lack** of investigation into the specifics of blockchain ***scalability, traceability, automation and other key factors*** (Enoch and Omijeh, 2023). They indicate that there is a lack of information on these specific characteristics of a decentralized database in the context of realistically choosing and implementing an optimal framework into a system, therefore indicating a research gap. However, with further research discussion in the *Literature Analysis: 4.2.2 Research Question 2* (p. 96), this argument is **challenged**.

In efforts to answer this question posed by the above researchers, in Siful Islam and Kutub Apu's (2024) research article, "Decentralized vs. Centralized database solutions in blockchain: advantages, challenges, and use cases", they indicate that while decentralized databases **excel** in enhanced security and transparency, they particularly **struggle** with scalability and efficiency - especially in scaled environments with increased transactions. The research article above is supported by Jesse Yli-Huumo et al.'s (2016) research article, "Where Is Current Research on Blockchain Technology?—A Systematic Review", **similarly** indicating that decentralized databases pose a challenge to its widespread adoption due to its **lack of performance scalability**. In a practical example to indicate the scale of transaction in cryptocurrencies, Bitcoin transactions take around 10 minutes to add a

block to the chain. A blockchain may only manage 7 transactions per second (tps). VISA can process 24 000, and Twitter with 5000 (Yli-Huumo et al., 2016).

Wang et al. 's (2022) research article, “vChain+: Optimizing Verifiable Blockchain Boolean Range Queries” indicates simply that organizations that focus on data security and transparency will favour decentralized databases. **However**, centralized databases may be chosen due to greater efficiency (performance and scalability). This is an important point which is further discussed in the *Literature Analysis: 4.2.2 Research Question 2* (p. 96).

According to Yakubov et al.’s (2018) research article, “A Blockchain-Based PKI Management Framework”, they explain functionality of a blockchain-based PKI. In conclusive testing results of their research, they indicate that the marriage of PKI and blockchain technology produced a pleasing and acceptable maintenance costs, as well as speedy performance and transaction rates.

In further research and discussion of Public Key Infrastructure (**PKI**) and Certificate Authority (**CA**) being used, and explored in conjunction with blockchain technology, according to Qurotul Aini et al. ‘s (2022) research article, “Blockchain Based Certificate Verification System Management”, indicates that ***certificate revocation management*** has **worsened** due to cloud computing and **T**he **I**nternet of **T**hings (**IOT**). While PKI’s are, according to their brief definition, a set system (foundation) with specific rules to control public/private key mechanisms, the mention of IOT’s had proven a significant point for the thesis when applied to broader contexts. **IOT**, according to Kinza Yasar and Alexander Gillis’s (2024) online definition, “internet of things (IoT)”, are **interrelated smart devices** that connect to a cloud or network that are aimed at **enhancing** the quality of life for humanity (personally or professionally). These typically embody sensors, mechanical and/or digital machines, and consumer objects. These include a pacemaker, holt monitors, biochip transponders in animals, smartwatches, security alarms, cashier product scanners etc.

Therefore, going back to Qurotul Aini et al. ‘s (2022) research article with **IOT’s** in mind, they indicate that there are many vulnerabilities due to **openness** and **connection** of **use cases**. **Cryptographic solutions** (blockchain technologies) may resolve some of these issues. In the authors' experimental research, they indicate a standard blockchain system had immense delay due to the system tracking location of transactions. In order to solve this issue, the author implemented a ***strategy*** with CRL distribution points in conjunction with a Bloom filter. While the intricacies of the research is out of the thesis’ scope, the overarching point that cryptographic solutions may resolve

interrelated smart devices sparks further discussion in the *Literature Analysis*: *4.2.1 Research Question 1* (p. 80).

2.2.3 Recognising Current Methods of Counterfeiting

Current counterfeiting methods would be beneficial to identify due to the ability to expose the problem area, identify key concepts within, elaborate details accurately and apply it to the context of the core research question. According to Aamna Tariq et al. 's (2019) research article, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System", global report statistics in 2013 indicated that corruption within education is a worldwide issue. It is also more prominent within developing countries, often taking the forms of bribery, nepotism in academic admissions and exam results, inappropriate use of funds, diploma mills, 'ghost schools' that are legally registered but have no evidence of legitimately existing, and external accreditation services (external moderation by a third party outside of an educational institution) that are compromised or corrupt. According to the article above, they indicate a list of current methods of counterfeiting (fraud):

Document fraud: A common counterfeit, where there is an alteration of **steganography.** Signatures, serial numbers, degrees and certificates (credentials), and any relevant additional details (seals and logos) are faked.
Institutional fraud: University records are backed up on the system, however, institution staff administrative roles may be compromised and corrupted. A third party (administration) may alter records on the system, and will be difficult to identify due to the possibility of innocent clerical errors.
Diploma Mills: A massive underground, worldwide black market that is extremely profitable and organized - often with sophisticated, dedicated corporate teams. These online '*mills*' take an extremely professional appearance, however, the universities are illegitimate and offer counterfeit degrees under '*digital custom products*'.
Accreditation Fraud: Often used in tangent with diploma mills, acting as a third party (external moderation) to authenticate fake credentials that are sold out (Aamna Tariq et al., 2019).

According to Bhekabantu Ntshangase and Steven Msosa's (2022) research article, "The role of the South African qualifications authority in curbing misrepresentation of qualifications", they also add onto the list:
Translations: Papers that are purposefully incorrectly translated, such as modification of course

names or grades. Logically, there would be some underlying internal syndicate, as there may be some illegal compromise between staff and students.

According to Tasfia Rahman et al.'s (2023) research article, "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS", there is evidence of multiple devoted fraudulent organizations that service and provide fake academic certificates to anyone who is willing to pay. As a result, with a **sheer amount** of records that fall into the academic systems, it is extremely time consuming, taxing and simply **difficult** to authenticate genuine academic credentials. This includes the application of students going into universities (National Senior Certificates), as well as graduates that may enter the workforce or apply for postgraduate studies. The paper indicates that blockchain is the way of the future, but it also offers a case study tool for a peer-to-peer network protocol called "The InterPlanetary File System" (**IFPS**). It streamlines external companies/organisations by allowing them to rapidly examine the authenticity of a certificate while also ensuring that graduates do not have to worry about a physical certificate becoming lost or damaged. The original credential certificate is stored on the **IFPS**, however the hash associated with the certificate is stored on the blockchain. As long as the digital database is operational (up and running), all information is forever digitized.

According to Seong-Kyu Kim's (2022) research article, "Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm", they emphasise - just like in Rahman et al.'s (2023) research article above - that eLearning is an important step towards a progressive Fourth Industrial Revolution, digitising certificates or diplomas as more higher education institutions issue credentials online. However, digitization affords **easier** windows of opportunity for forgery, counterfeit and compromisation of digital systems (hacking). Uniquely, the article proposes that the help of **artificial intelligence** may be used to assist with **digitization issues** that Rahman et al. presented. According to Seong-Kyu Kim, they build on the idea with an additional proposition that is made where **algorithms are needed** to encrypt credentials using hash functions, converting data with different lengths of hash functions into data with fixed lengths - as explained in *Literature Review*: 2.2.1 *Methods of Online Authentication* *(p. 26)* above. This serves as proof that other sources support the thesis' proposition, **however**, there was a key point in the article where it indicated that institutions would have to invest a large sum of money, time and resources (labour-intensive) into converting old, physical credentials of past students into digitized versions. This is a **vital consideration** if South Africa were to begin implementing a decentralised database within their higher education institutions. A suggestion to this idea, indicated in the article,

interestingly gives **Artificial Intelligence** the spotlight, in the form of 'Artificial Intelligence Consensus Algorithms', a **marriage** between hash functions and artificial intelligence. (Indicate that artificial intelligence is an algorithm that follows the rule every single time without a third party, therefore cannot be that easily maliciously manipulated). Artificial intelligence may also help with "***selective management of necessary data***" (Kim, 2022).

In support of Seong-Kyu Kim's (2022) research article, Joanna Black and Cody Fullerton's (2020) journal article, "Digital Deceit: Fake News, Artificial Intelligence, and Censorship in Educational Research", also emphasize that we simply **cannot** regress back in time to old methods of document authentication (physical steganographic characteristics). This is especially in the context that **educators must be made aware of disinformation and misinformation**, as the internet offers a vast expanse of information and the vast progression of artificial intelligence, illegitimate research and current counterfeit methodologies. Joanna Black and Cody Fullerton's point supports the section of the *Literature Review*, as conducting research on this topic intentionally brings awareness to the reader as well as explores possible solutions to an important problem.

In the *Literature Analysis*: *4.2.1 Research Question 1* (p. 80) section, the above research indicates that blockchain offers such a potential to get rid of all these problems. It can be devoid of an aggressively progressive technology such as artificial intelligence, **ironically** use artificial intelligence as a method of implementation to solve problems that require algorithms, eliminate illegal black markets and provide a secure environment for educational institutions which holds its academic integrity.

2.2.5 Socio-Economic Causes of Digital Counterfeiting

There is clear evidence, according to Aamna Tariq et al.'s (2019) research article, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System", that **developed** countries serve as the main largest supporting industries for underground credential forgery markets, including **China**, the **United Kingdom** (**UK**) and the **United States** (**US**) being one of the biggest contributing culprits. Therefore, in the above research article, they indicate that there is an increased competition within job markets, including moderate to low skill positions, that are overly-relying on credentials within an extremely expectant culture of credentialism within the 21st century modern society.

The South African Perspective

Therefore, applying this to the South African context, according to Lonias Ndlovu and Andrew Leslie's (2022) research article, "False or Fake Qualifications in an Employment Context: A South African Perspective", they indicate that there is clear pressure for employment and/or a promotion - aimed for **additional monetary bonuses**. It causes an overall rise to competition within the job market. In this way, it simultaneously **causes** a socio-econonic issue; the person who is hired with a fake qualification will be underskilled and do potentially **immense** ethical and irreversible harm, especially jobs that require critical skills and expertise (such as medical care).

According to Bhekabantu Ntshangase and Steven Msosa's (2022) research article, "The role of the South African qualifications authority in curbing misrepresentation of qualifications", they indicate statistics within South Africa that in six of the nine provinces, there is more than 50% of the employed that have level of education is **below** matriculation. According to Statistics South Africa's (2016) report, **58.8%** of jobless individuals had less than a matriculation certificate, followed by **32.4%** having a matriculation certificate. With this information within Bhekabantu Ntshangase and Steven Msosa's (2022) research article, we can evidently assume that there is a **high motivation** for the use of fraudulent credentials. **Credentialism** has also been mentioned in the above paragraph, supported by the previous Aamna Tariq et al.'s (2019) research article, that there is a general idea that the **higher the degree of the candidate, the more the employer will be associated with desirable qualities within the workplace (devotion, abilities, dependability, talent).** Due to the negative impact of the cultures of credentialism, fraud is seen as justified to some people who believe that companies are unjustly **denying** them job opportunities or promotions due to a lack of higher education credentials, information supported by Guernsey (1997). This point is extremely valid, despite the year of publication.

The paper above also indicates that there is a need for a more ethical conduct of staff within a higher educational institution. However, with the benefit of blockchain technology, many of the problems may be eliminated or reduced. This point is further discussed in the *Literature Analysis: 4.2.1 Research Question 1* (p. 80).

2.3 Educational Resources

How can blockchain technology be used to introduce valuable educational resources? What are the benefits and drawbacks, as opposed to current day existing resources?

Introducing the topic and placing it in its historical context, it is clear that the rapid progression (*and succession*) of digital technologies produced a **domino effect** within the (broadly and previously mentioned) operations of governance, business, education and civilian life. Interestingly, it is also important to note that it is a **natural** progression of history and time, thinking back to a very simple example; A small village spreading news via word of mouth evolved into the introduction of newspapers. Then, the explosion of television (consumerism and appliances) allowed for news channels to verbally and visually communicate to a massive audience through the convenience of their homes. In the 21st century, the emergence and convenience of online shopping and banking **required** techniques of online authentication to assure **safe** digital payments, preserve identity, and develop and implement counter-measures to ever-advancing criminal methodologies.

In basic knowledge, all people living in the 21st century understand that universities and higher education institutions have also implemented digital services as a result of this **domino effect** mentioned in the above paragraph. Notably, the implementation of digital services were also greatly accelerated due to the outbreak of COVID-19 in 2020, according to Shivangi Dhawan's (2020) online research article, "Online Learning: A Panacea in the Time of COVID-19 Crisis", which explains one of the many forced changes that occurred during the pandemic, specifying mostly into the pedagogical approach of traditional face-to-face teaching and learning **adapting into** e-learning.

Focusing back to the concept of credibility and validity of digital movement within an educational institution, according to Fawaz Habbal's (2023) journal article, "The Implications and Efficacy of Online Verification Tools inScientific Research and Citation Practices", they explain that the explosion of digitized, freely-available online research has **necessitated** technologies that have the ability to verify and give **credibility** to academic articles. In their recommendations for future research, they emphasize the need for further research to develop and refine **algorithms** that may be able to identify academic misconduct and streamline peer-reviews. Additionally, they touch on

the aspect of **longevity**, a desire for a tool that may provide a long-term positive impact on "*scientific integrity, research productivity and scientific literature*" (Habbal, 2023).

Thus, to apply further security research in light of Fawaz Habbal's (2023) journal article, mentioned in the above paragraph, it would be necessary in the thesis to identify the possible solutions for the desired academic tool. This tool proposed is obviously using the benefits of blockchain technology to check off these desirable traits. It is important to indicate that this section of the Chapter **deviates** from foundational theory, instead **identifying and evaluating current sources** to further strengthen the *Literature Analysis*: 4.2.2 *Research Question* 2 (p. 96) as the core research questions are answered with such evidence.

2.3.1 Examples of Existing Blockchain Databases

In support of the thesis proposal of utilizing blockchain technology within a higher education institution, the examples below are trusted sources which indicate existing blockchain databases that have indicated their utilization of blockchain technology in order to assist with credential authentication.

The University of Central Asia (**UCA**)
https://ucentralasia.org/schools/registrar/degree-verification
Graduates ascending from The University of Central Asia (UCA) are provided a paper-based degree, as well as a digital version on their own blockchain database system. In the above-provided link, it is a direct example which shows a **user-friendly, publicly-accessed** online webpage. An external potential employer may upload a PDF of the graduate's credential document directly onto the website, and results will deem it valid or not. There is no need to contact the facility for verification, saving time for all parties involved. They **do not** disclose the details of how their blockchain database operates.

Massachusetts Institute of Technology (**MIT**)
https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017
According to Elizabeth Durant and Alison Trachy's (2017) online article, "Digital Diploma debuts at MIT", they indicate that the Massachusetts Institute of Technology had utilized an application called **'*Blockcerts Wallet*'**, developed in collaboration with **Learning Machine** and their internal MIT

Registrar's Office. This article is published directly on the institution's website, openly sharing information on understandable explanations of how this blockchain database works in favour of their institution. They indicate that in their usage of blockchain technology, merely the time-stamped transaction of when MIT produced the record, a **sensible** implementation of this technology as it still validates a credential. Furthermore, having a blockchain database system in the form of an application is clearly designed to be as user-friendly as possible, offering graduates autonomy of their credentials and being able to share them freely with others without the risk of security concerns. As an interesting point to take away from this information, the article describes the clear functionality and reasoning of their choice in implementing a blockchain database system, highlighting that their focus is on the desire of credential record longevity, and introducing the concept of a new ***meta-record***. They indicate that blockchain technology has **enormous** potential in pushing academic boundaries, as well as external businesses already opting for the benefits within their own organizations.

The University of Melbourne

https://www.unimelb.edu.au/newsroom/news/2017/october/university-of-melbourne-to-issue-recipient-owned-blockchain-records

Interestingly, The University of Melbourne **also** worked in collaboration with (open-source code) **Learning Machine (*'Blockcerts'*)**, according to their (2017) direct webpage article, "University of Melbourne to issue recipient-owned blockchain records". They discuss the same things that are addressed in Elizabeth Durant and Alison Trachy's (2017) online article. However, they also add an interesting point that if an institution shuts down, credentials are still saved on **'*Blockcerts*'**, indicating **longevity** that is validated on an accredited third party.

City University of Paris

https://cityuparis.fr/credentials-on-blockchain/

The City University of Paris, according to their (2023) website article, "Credentials on Blockchain", indicate that Awards may be validated using the easy accessibility of a Quick Response (**QR**) code. Vaguely, they explain that the QR code will take the user to the webpage where they may be able to verify the credentials. They **do not** go into detail about how their blockchain database system operates, instead highlighting the advantages of one.

University of Johannesburg

https://news.uj.ac.za/news/uj-implements-blockchain-based-certificates-for-graduates-2-2/

According to the University of Johannesburg's (2022) website article, "UJ implements Blockchain-based Certificates for graduates", **also utilizes QR codes** which leads to a webpage to validate credentials. They do not go into detail about how their blockchain database system operates, instead highlighting the advantages of one, and the fact that it was the **first university in South Africa** to incorporate blockchain technology security features to their credential record systems.

2.3.2 Current States of Existing Blockchain Databases: Are they successful? Useful?

Due to a lack of quantitative data, this core research question could not be appropriately answered. However, this had been kept in the thesis due to its impactful implications and discussion within the *Literature Analysis: 4.2.2 Research Question 2* (p. 96).

Chapter 3: Methodology

3.1 Introduction

The intention of this section is to explicitly elaborate on the elements of Saunder's et al.'s Research Onion, following Choice, Framework, Approach, Philosophy, Data Collection Procedures, Data Analysis, and Limitations, Validity and Reliability in the applied context of this thesis.

The analysis primarily uses examples from international and local **case studies** to estimate the success of specific blockchain implementations within their institutions, as well as identify and fill a **research gap** (identified through the *Literature Review: 2.1.2 The Research Gap within South Africa* (p. 20-21) section of this proposal paper) within the context of South Africa and its higher education institutions. Thus, it is important to note that this thesis understands South Africa's socio economic issues, and how results may potentially differ when implemented in other countries. This generates the idea of an unexpected phenomenon, which is significant in choosing the most ideal research methodology. However, this will be discussed further in this portion of the study. Ultimately, this demonstrates the **reasoning** and **need** to further explore this under-researched topic within the localized (South African) context.

3.2 Choice

The study aims to research **qualitatively** how blockchain technology may improve higher education, focusing on security, validity, and educational resources within the boundaries of the South African context. As previously and briefly mentioned in the *Introduction: 1.4 Problem Area* (p. 11) of this paper, there is **insufficient information** to choose which experiments or what primary data collection to do, thus, qualitative case study research needs to be conducted. As a result, *Saunder et al.*'s popular *Research "Onion" Framework* was selected because of its advantages, which Aleksandras Melnikovas's (2018) online journal article, "Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies", elaborates and explains more clearly. They emphasize that the Research "Onion" Framework offers immense **flexibility** which enables the researcher to select a variety of the most suitable **theories** or practises (unconstricted to one field or discipline) that align with the needs and goals of their paper, offering coherent structure as a result of the layering system within the methodology. Simultaneously, the layering system ensures critical thinking and logical consistency as it, contextual to this thesis, follows a deductive approach and streamlines a larger theory into critical analysis and theoretical application towards the core research questions.

Other approaches may be regarded as appropriate for the thesis, although they are not as suitable as the Saunder's et al. 's Research ``*Onion*" *Framework*. For example, *Creswell and Creswell's Framework*, explained in John Creswell and David Creswell's (2017) book, "Research design: Qualitative, quantitative, and mixed methods approaches", elaborates on the choice of three types of design, qualitative, quantitative and mixed methods of research gathering. Saunder's et al.'s *Research ``Onion" Framework* is favoured because of its **linear** methodical (step-by-step) approach, the researcher's preference for a chronological thinking style, ease of usability and understanding for a novice seeking direction, as well as offer a **deductive** approach - which is crucial when dealing with a broad research question that must be narrowed down.

3.3 Framework

Saunder's et al.'s *Research ``Onion" Framework* is chosen as a base structure, as it gives a clear, visual overview of the methods taken to validate the research conducted.

It is outlined visually using Saunders et al.'s "Onion" framework, as seen in *Figure 10* below.

3.3.1 Saunder et al.'s Research Onion

***Figure* 10**

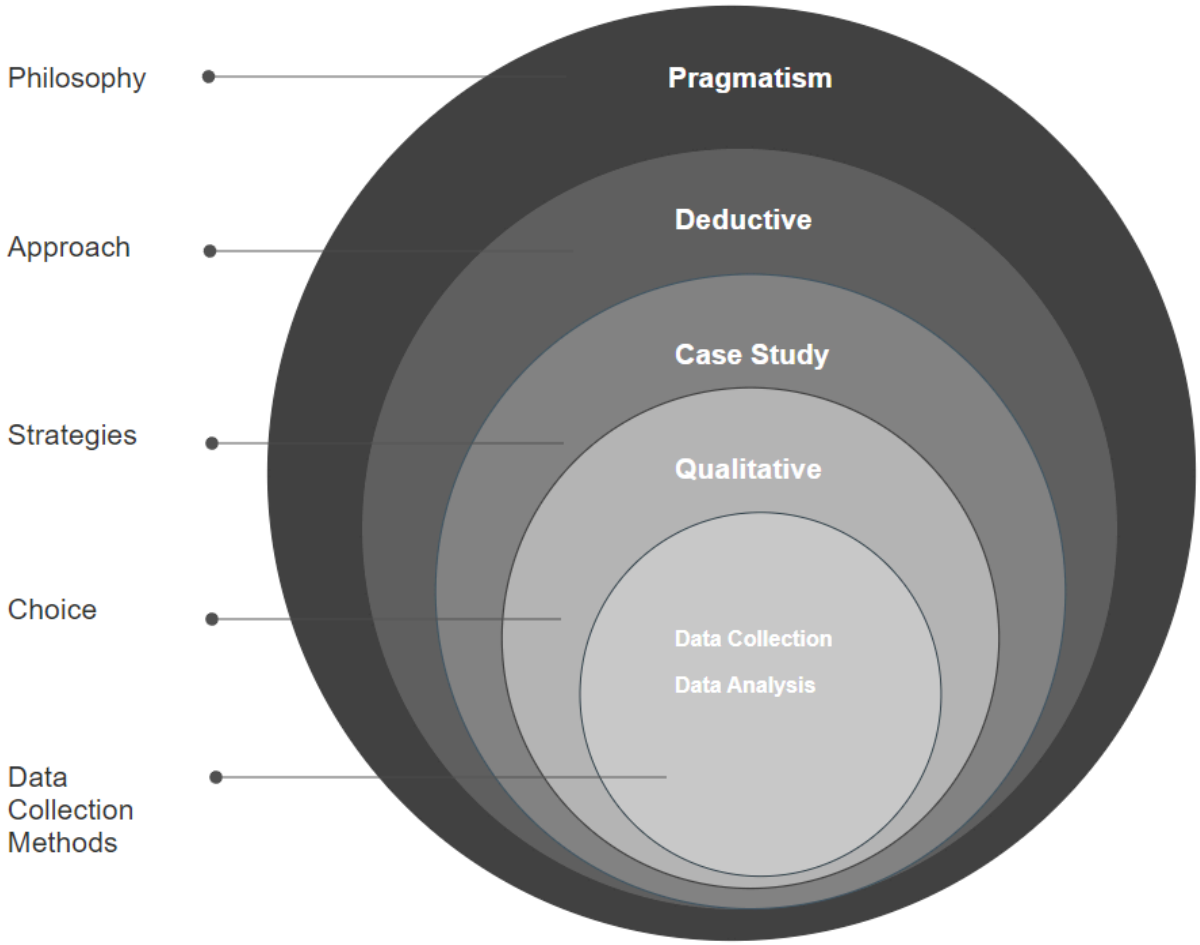


Figure 10: *The Saunder's et al.'s Research "Onion" Framework (Saunders et al., 2009), adjusted in the context of this thesis.*

3.4 Strategy and Approach

The Case Study approach, according to Crowe et al.'s (2011) journal article "The case study approach", explains the ability for case studies to enable researchers to explore *in-depth, multi-faceted complexities*. This is appropriate for this thesis since there are several research questions with their own unique features and *understudied phenomena*. These questions are proposed in the *Chapter 1 Introduction*: 1.3 *Aim* (p. 7) section of this paper.

It serves as a flexible and valuable instrument, as it importantly **emphasises** the **quality, integrity** and **validity** of informational sources. As initially stated, the thesis is subjected to a **qualitative** research approach that incorporates **thematic** data analysis, ideally, seeking understanding and patterns across a significant number of conveniently, open-source, freely available external online informational resources. Frequently accessed academic, digital databases include Google, Google Scholar, Research Gate, arVix, and ScienceDirect.

In addition, a **deductive** form of analysis (or informally known as the *top-down approach*) is used as a methodology within expected themes to approach the presented research questions in this study. It is ideal in this thesis to use as many components as possible to reach a final conclusion on each research question. According to Jaana Woiceshyn and Urs S. Daellenbach's (2018) article "Evaluating Inductive versus Deductive Research in Management Studies: Implications for Authors, Editors, and Reviewers", deduction is moving from the general to the particular, having a starting theory, theorise and evaluate said theory and finally adjusting and refining the theory according to what information was found. This is advantageous to this thesis since several micro-research questions have been gathered to potentially identify and validate the adoption of Blockchain technology into higher education.

Additionally, it is significant because micro-research questions provide a comprehensive analysis of the research collected (literature, case studies, and qualitative software test results) and enables an intimate familiarity with the academic context of the thesis and its theory applied coherently to the research question. Forming an established, theoretical framework within the Literature Review generates and assigns initial codes/labels/tags that represent relevant concepts, and is able to be referenced throughout the thesis and apply to the core research question. With the generation of codes/labels/tags, such as the example of the '*Understudied Phenomena*' or , it can be continuously referenced throughout the thesis and simultaneously group ideas and identify common **themes**. Themes are able to be reviewed and refined.

3.5 Philosophy

This thesis adapts to the Pragmatism philosophy. According to Douglas McDermid's (2023) online article "Pragmatism", research is accepted once there are substantial and satisfactory practical

components to support it. According to the context of this thesis, this research philosophy is used as a way to interpret what "*works best*" and allows the researcher **flexibility** in their approach to the research. Stated by Leanne M Kelly and Maya Cordeiro's (2020) online journal article, Pragmatism may move beyond conceptualization, emphasising the retrieval of knowledge and inquiring its practical usage.

3.6 Data Collection Procedures

As previously stated, the thesis is focused on a **qualitative**, **case study** approach to data collecting, with **no** intention of experimentation and primary data collection. According to Paradis et al.'s (2016) journal article, "Design: Selection of Data Collection Methods", *textual or content analysis* can vary within the amount and type of papers sourced are determined by the research questions. It helps give contextualization from written reflections of other researchers.

A table with all the key research questions have been assembled, along with the exact desired information sampling sources and techniques.

Case studies and their selection process is as follows;
- Has been published within the last 5 years. If this exceeds, there needs to be an accompanying explicit reasoning why.
- An open sourced accredited research database searching through Google Scholar, ScienceDirect, ResearchGate and arXiv e-Print Archive favoured.
- Case studies of real life events are checked through reliable news reporting websites online.

Research Variables and Methodology	
Security and Validity	
Research Variable	**Methodology**
• Determine methods of Online Authentication of Legal Documents	- Online **case studies**, websites offering online services - International **and** South African context
• Compare closed, centralised database to a Blockchain database	- Assemble and correlate online information (comparison) - Documentation collection
• Recognizing Current Methods of Counterfeit	- Multiple sources of academic information (articles, journal publishings) to identify **common patterns (thematic analysis)** - Verifiable online news outlet reports (2019 to 2025) - Local (South African) context - Documentation Collection
• Identify Gaps in Typical Security Technology	- Verifiable online news outlet reports (2020 to 2025) - International Context
• Identify Socio-Economic Causes of Counterfeit	- Verifiable online news outlet reports (2020 to 2025) - Online journal articles - Local (South African) context

Educational Resources	
Research Variable	**Methodology**
• Compare Utility within Regular Databases vs Blockchain Databases	- Assemble and correlate information (comparison) - Online **case studies**, websites offering online services
• Provide Examples of Existing Blockchain Databases	- Assemble and correlate online information (comparison) - Online **case studies**, websites offering online services (international and/or local context)
• Pursue Information about Existing Blockchain Databases: Are they successful? Useful?	- Online **case studies**, websites offering online services (international and/or local context)

3.7 Limitations, Validity and Reliability

According to Vaismoradi et al.'s (2013) journal article, "Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study", a **flexible** research approach, such as Saunder's et al.'s *Research ``Onion" Framework*, may lead to inconsistency, typically giving an unfocused, incoherent, generic viewpoint. **Ethnography** may play a vital role in informative sources, as **internationally sourced** online research was carried out in numerous contexts including various socioeconomic issues that may be completely different to South Africa. As a result, it is critical to carefully select informational sources that give the highest quality and most applicable evidence to highlight points, support the presented hypothesis, and apply it to the primary research questions.

Furthermore, the article "Blockchain-Based Applications in Education: A Systematic Review" by Alammary et al. (2019) proposes the concept of validity threats through **researcher bias**. In the context of this thesis, it is mainly evident that it is actively searching for positive arguments prior to negative ones. Through unreferenced communication within the article, Fred Hess recalls that *validity is something of integrity of the researcher, and not the result of indifference* (Alammary et.al,

2019). By being transparent and explaining researcher bias within this paper particularly, it gives a clear indication of intention of the research.

Researcher bias has previously been mentioned in the introduction of this proposal, as well as there are shards of it found throughout the paper. This is intentionally written purposefully to alert the reader that there is awareness of this factor, especially within the nature of the research. The most ideal way of dealing with validity threats can come in the form of **comparison** between informational sources and **identifying** and **analysing discrepant data (**Alammary et al. 2019). These strategies bleed into each other, as when identifying and analysing discrepant data may be in the form of external feedback, as well as comparing multiple sources with each other. Alammary et.al's (2019) article supports Vaismoradi et al.'s (2013) journal article, as both imply that to support credible research, the most consistent evidence must be found. This is specifically addressed in the methodology research framework as Data Collection and Data Analysis.

In the context of reliability and the nature of this particular quantitative research, the speed at which technology is developing, and the inevitability of outdated technologies mean that subsequent research may not provide the exact same findings (Saunders et al., 2003). Therefore, the research is aware and transparent that it is clearly capturing the time period.

Chapter 4: Results & Literature Analysis

This chapter presents the research findings in a straightforward and systematic manner, revealing case studies and patterns that developed from thematic analysis. The chapter begins with the findings, which are presented clearly and summarised in the appropriate format of tables and ordered lists. With the presentation of factual information in the results, the literature analysis goes beyond and offers engagement, exploration and deep analysis with the information, identifying contradictions, inconsistencies, unexpected outcomes, patterns and thoughtful interpretations of the results. This section also aims to show a balanced understanding by offering alternative explanations for findings. The literature analysis applies key contributions of study to the field, applying how the research conduct addresses the gap in the literature that was identified in the *Introduction*, providing new insights and broader implications of the findings. There is an additional implication of how beneficial the research may be outside of higher education institutions within South Africa.

4.1. Results

Results are organised by the two core research questions of the thesis, *how blockchain technology can be used to secure and validate educational credentials* and *how blockchain technology can be used to introduce valuable educational resources, and how it compares to present resources.* Information is presented systematically in the form of **one** table, with paraphrased and simple summaries. Due to the nature of the key research findings, the large scale of information and the fact that research bleeds into each other, the table is unified to allow ease of cohesion and readability. Therefore, the table had not been alphabetically ordered in favour of a numerical order, due to symbiotic research.

4.1.1 Research Question 1

How can blockchain technology be used to secure and validate educational credentials?

Finding 1.1

Increased security and tamper-proofing

Finding 1.2

Streamlined verification process

Finding 1.3

Changes in implementation

4.1.2 Research Question 2

How can blockchain technology be used to introduce valuable educational resources, and how does it compare to present resources?

Finding 2.1

How blockchain technology may be used to introduce valuable educational resources

Finding 2.2

Present implemented blockchain resource

Table 2

Below are the research findings in a table format, as well as a presented colour-coded key for ease of readability.

Table 2: Key

Finding 1.1	Increased security and tamper-proofing
Finding 1.2	Streamlined verification process
Finding 1.3	Changes in implementation
Finding 2.1	How blockchain technology may be used to introduce valuable educational resources
Finding 2.2	Present implemented blockchain resources

No.	Author/s, Publication Type and Title	Year	Key Finding/s	Finding 1.1	Finding 1.2	Finding 1.3	Finding 2.1	Finding 2.2
1	Guang Chen, Bing Xu, Manli Lu & Nian-Shing Chen's article," Exploring blockchain technology and its potential applications for education"	2018	**Indicating** a research gap whereas insufficient blockchain research, and studying themes on future educational revolutions, would be challenging. The research article's year of publishing gives an important baseline of comparison, from 2018 to (current year) 2025.			Changes in implementation	How blockchain technology may be used to introduce valuable educational resources	
2	Alammary et al. research article, "Blockchain-Based Applications in Education: A Systematic Review"	2019	**Focusing** on identifying multiple research papers that have been published, and studies that have been conducted, in the context of implementing blockchain technology into educational institution systems. Indicating a growing interest in investigating the potential of blockchain technology. However evidence points to prematurity and within theoretical speculation. This also gives an important baseline of comparison, from 2019 to (current year) 2025.			Changes in implementation		
3	Grigore Albeanu's research article "Blockchain technology and education"	2017	**Explaining** that blockchain is engineered in such a way that guarantees transaction irreversibility, prevention of counterfeiting and double spending. **Indicating** blockchain technology will be useful for new pedagogy, meta-university introduction with student contracts and student records.	Increased security and tamper-proofing	Streamlined verification process	Changes in implementation	How blockchain technology may be used to introduce valuable educational resources	
4	Guang Chen, Bing Xu, Manli Lu & Nian-Shing Chen's article, "Exploring blockchain technology and its potential applications for education"	2018	**Illustrating** the idea of education institutions using system reforms to accommodate positive online learning experiences; implementing student achievement validation databases, digital currency as a form of student credit as well as the concept of smart contracts.		Streamlined verification process	Changes in implementation		

5	Dineo A. Matlebjane and Patrick Ndayizigamiye's research article, "Antecedents of the adoption of blockchain to enhance patients' health information management in South Africa"	2022	**Providing** a similar case study in the context of South Africa; identifying the validity of blockchain technology and its potential positive impact on system operations and data management.			Changes in implementation		
6	Guangyuan Chen's research article, "Optimizing Digital Signatures for Enhanced Privacy Protection in Blockchain Systems"	2024	**Explaining** that blockchain technology may greatly prevent unauthorised access to extremely sensitive data. Data can be exchanged between organizations while maintaining privacy. Indicates that blockchain technology can be useful to various aspects of the supply chain.	Increased security and tamper-proofing	Streamlined verification process	Changes in implementation	How blockchain technology may be used to introduce valuable educational resources	
7	National Department of Health's journal, "National Digital Health Strategy for South Africa, 2019 - 2024",	2012	**Seeking** to develop and provide a national, digital platform for storing healthcare data on patients, medicine, and human resources.			Changes in implementation		
8	World Health Organization's (WHO) webpage, "National Digital Health Strategy for South Africa 2019-2024"	2019	**Indicating** that the nine strategic interventions had stated that the implementation of the digital health platform is to be completed by 2024.			Changes in implementation		
9	BizCommunity's online article, "#BizTrends: NHI to boost South Africa's digital healthcare"	2024	**Stating** that it is still in progress and is closer to completion. As of the 27th of February, the time this article was published and at this point of the thesis, there have been no further reports.			Changes in implementation		

10	Cape Town Today's webpage, "South Africa's Digital Transformation: A Leader in E-Government Development" by Isabella Schmidt	2024	**Providing** evidence of an additional successful initiative within South Africa to progress and improve government services by digitising physical lineups which provides evidence on progression moving forward into the 4th Industrial Revolution.			Changes in implementation		
11	https://www.ekurhuleni.gov.za/	2025	**Indicating** a practical example and evidence that South Africa is moving forward into the 4th Industrial Revolution.			Changes in implementation		
12	Akinradewo et al.'s research article, "A principal component analysis of barriers to the implementation of blockchain technology in the South African built environment"	2022	**Identifying** the general boundaries that South Africa has to implement such technology, such as technological obstacles and reiteration of old systems - which is time consuming and costly (resource and labour intensive). Especially for funds and adequate, trained staff.			Changes in implementation		
13	Steven Leibson's online article "Blockchain is not Bitcoin—Bitcoin is not Blockchain"	2018	**Stipulating** the misunderstanding of blockchain being defined with direct association to Bitcoin and NFTs.			Changes in implementation		
14	Shivangi Dhawan's online research article, "Online Learning: A Panacea in the Time of COVID-19 Crisis"	2020	**Explaining** that digital services was one of the many forced changes that occurred during the pandemic, specifying mostly into the pedagogical approach of traditional face-to-face teaching and learning transforming and adapting into e-learning.			Changes in implementation		
15	Fawaz Habbal's journal article, "The Implications and Efficacy of Online Verification Tools	2023	**Identifying** a research gap, problem statement and thesis direction, indicating there is a need for developed and refined algorithms that are able to identify academic misconduct, with a long-term positive impact "scientific integrity, research productivity and scientific literature" (Habbal, 2023).	Increased security and tamper-proofing	Streamlined verification process	Changes in implementation		

	inScientific Research and Citation Practices"							
16	Mathe et al.'s journal article, "Securing Information: Cryptography and Steganography"	2012	**Indicating** a direction of the thesis; that cryptography offers "*security science, ensuring privacy, integrity of data, entity authentication, and data origin authentication*" (Mathe, R, et al., 2012).	Increased security and tamper-proofing	Streamlined verification process			
17	Paul Krzyzanowski's (2024) online article, "Steganography & Watermarking"	2024	**Critical foundational theory**. **Explaining** the purpose of cryptography is that the contents of a message is concealed.	Increased security and tamper-proofing				
18	Alenezi et al's journal article, "Symmetric Encryption Algorithms: Review and Evaluation study"	2020	**Critical foundational theory**. Both encryption and decryption is done using a singular key, and is often referred to as a secret key, as it is kept in a secure channel, as clearly described.	Increased security and tamper-proofing				
19	Yehuda Lindell's (2007) book, "Introduction to Modern Cryptography: Principles and Protocols"	2007	**Critical foundational theory**. **Explaining** a simple process of Symmetric (Private) Algorithms; key-generation (1), the encryption (2) and the decryption (3).	Increased security and tamper-proofing				
20	Johnathan Bevers's (2021) thesis, available online as open-source academic material, "The Study of Symmetric and Asymmetric Key Encryptions"	2021	**Critical foundational theory**. Due to the explanation of Symmetric (Private) Algorithms above, the introduction of Asymmetric (Public) Algorithms indicates that it solves its Private Algorithm issues, such as needing additional security on documents/applications. Explains functionality of Asymmetric Algorithms in the context of a NFT (a blockchain-based digital asset).	Increased security and tamper-proofing				

21	Rajeev Sobti and Geetha Ganesan's (2012) journal article, "Cryptographic hash functions: a review", and Qing Zhou et al.'s research article, "Quantum-inspired Hash Function Based on Parity-dependent Quantum Walks with Memory (August 2023)"	2012 and 2023	**Critical foundational theory**. **Indicating** information on hash functions, which is a mathematical algorithm, offering a solution to ensure "digital identification, message authentication, digital signatures and pseudorandom number generation" (Qing Zhou et al., 2023). **Both** research articles here support the same information provided in Johnathan Bevers's (2021) thesis.	Increased security and tamper-proofing				
22	Sungbeen Kim and Dohoon Kim's (2024) research article, "Data-Tracking in Blockchain Utilizing Hash Chain: A Study of Structured and Adaptive Process"	2024	**Critical foundational theory**. **Explaining** functionality of hash functions (or hashing), with a definitive characteristic of expecting the mathematical algorithm to always output a fixed-size value regardless of input length. The output is then recorded on a fixed hash train, which is immutable and prevents any tampering.	Increased security and tamper-proofing				
23	GeeksforGeeks, online webpage	2022	**Critical foundational theory. Indicating** that the output of a fixed-size value is commonly called the hash value.	Increased security and tamper-proofing				
24	Shashwat Sharma and Ayush Mishra's (2024) research article , "A Comprehensive Study of Cryptographic Hash Functions", and Marut Pandya's (2024) research article, "Performance Evaluation of	2024	**Critical foundational theory. Explaining** that one minor change to the input variable will drastically change the output variable (hash value). Indicates that hash functions are trustless, immutable, automatic and secure, as there is therefore no central authority.	Increased security and tamper-proofing				

	Hashing Algorithms on Commodity Hardware"							
25	Qing Zhou et al.'s (2023) research article, "Quantum-inspired Hash Function Based on Parity-dependent Quantum Walks with Memory (August 2023)"	2023	**Explaining** that hash functions have theoretically infinite possibilities of the initial state and the irreversibility of modulo operation" (Qing Zhou et al., 2023). Hash functions are developed to distinctive needs.	Increased security and tamper-proofing				
26	GeeksforGeek's online website article, "Blockchain Hash Function"	2022	**Describing** and indicating a range of classes of hash functions; including RACE Integrity Primitives Evaluation Message Digest (RIPEMD), Message-Digest Algorithm (MDA), BLAKE2, Whirlpool and Secure Hashing Algorithm. Evidence of multiple choices for when developing a blockchain-based system within a higher education institution.	Increased security and tamper-proofing				
27	Shashwat Sharma and Ayush Mishra's (2024) research article , "A Comprehensive Study of Cryptographic Hash Functions"	2024	**Indicating** that SHA-256 is mostly used in blockchain technology due to the optimized balance between performance and security in comparison to other hash functions. SHA-3 is the most current and modern version, and applies to digital applications that need additional exceptional high security. **Explaining** that each block on the blockchain contains a hash of the previous block, forming an impossibly adjustable chain.	Increased security and tamper-proofing				
28	Guangyuan Chen's (2024) research article, "Optimizing Digital Signatures for Enhanced Privacy Protection in Blockchain Systems"	2024	**Explaining** a private key using a cryptographic mathematical algorithm to generate a digital signature. Further detailing into digital signature, which is used for the purpose of ensuring authentication, integrity and prevention of repudiation - imitating the concept of a real-life stamped fingerprint.	Increased security and tamper-proofing	Streamlined verification process			
29	Wei Bi, Xiaoyun Jia and Maolin Zheng's research article, "A Secure Multiple	2018	**Explaining** that ECDSA (Elliptic Curve Digital Signatures) digital signatures may both symbiotically use public key cryptography and hash functions. Bitcoin uses ECDSA to authenticate	Increased security and tamper-proofing	Streamlined verification process			

	Elliptic Curves Digital Signature Algorithm for Blockchain"		transactions, additionally renowned in its 30% increased algorithmic speed and efficiency in comparison to other curves.					
30	Guruprakash Jayabalasamy and Srinivas Koppu's (2022) research article, "An empirical study to demonstrate that EdDSA can be used as a performance improvement alternative to ECDSA in Blockchain and IoT"	2022	**Indicating** the historical slow technological transition of the digital signature from RSA to DSA to ECC (Elliptic Curve Cryptography). The successor of ECC is an EdDSA (Edwards Curve Digital Signature Algorithm) that shows, through testing, its robust performance, quick arithmetic, and resistance to hash collisions. However, a final point the article highlights is that EdDSA and ECDSA usage is case-dependent.	Increased security and tamper-proofing	Streamlined verification process			
31	Deepanshu Rana's journal article, "Advancements and Comparative Analysis of Digital Signature Algorithms: A Review"	2024	**Bringing** up the point of standardization in an example of the efforts of the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI), whereas there is an attempt at frameworking a chosen 'post-quantum cryptographic algorithm' that meets certain criteria for certain protocol. Sparks discussion within the Literature Analysis.	Increased security and tamper-proofing				
32	Liz George and Jubilant Kizhakkethottam's (2021) research article, "A Comparative Study of Zero Knowledge Proof and Homomorphic Encryption in Guaranteeing Data Privacy in	2021	Guangyuan Chen's (2024) research article, "Optimizing Digital Signatures for Enhanced Privacy Protection in Blockchain Systems included: Both the previous two research articles discuss zero-knowledge proofs and homomorphic encryption to be the most major solutions to this problem (privacy problems and improving digital environments). **Explaining** zero-knowledge proof, which is when evidence of the transaction is provided, however not leaking sensitive information. Homomorphic encryption is explained as the data being able to be worked with in its ciphertext without it being decrypted. Only the private key-holder will be able to decrypt the information and understand it.	Increased security and tamper-proofing				

	Blockchain Applications"							
33	Haque et al.'s research article, "An Innovative Approach of Verification Mechanism for both Electronic and Printed Documents"	2020	**Identifying** multiple methods of digital document protection. These include "digital watermarking, steganography, digital signatures and blockchain". Critical foundational theory. Steganography is defined, which sparks discussion within the Literature Analysis.	Increased security and tamper-proofing				
34	Margie Semilof and Casey Clark in Tech Target's website "steganography"	2023	**Critical foundational theory. Indicating** that steganography is aimed at hiding data in various complex ways. It is similar to cryptography as both are engineered to secure data; however, what distinguishes steganography from the latter is that it conceals the fact that the file has been encrypted with hidden messages. Data is encrypted into files such as JPEG images, audio or video files. When done correctly, files will look no different to the original.	Increased security and tamper-proofing				
35	Luca Caviglione and Wojciech Mazurczyk's research article "Never Mind the Malware, Here's the Stegomalware"	2022	**Critical foundational theory**. Malware is a broad definition, form of steganography. Its complexity deters the thesis into focus on cryptographic security science instead.	Increased security and tamper-proofing				
36	Rabia Tahir's (2018) article "A Study on Malware and Malware Detection Techniques"	2018	**Researching** into forms of technology weaknesses. This is narrowed down to viruses, worms, trojan viruses, spyware, adware, ransomware and rootkit, sniffers, keyloggers, phishing, spam. This is important as it sparks discussion within the Literature Analysis, determining contextualization within blockchain technology and reduction of phishing scams.	Increased security and tamper-proofing				
37	Marie Look's (2011) online article, "How to Add a Watermark to Photos"	2011	**Critical foundational theory. Discussing** watermarking in the traditional sense, which is when documents are held up to the light to assess whether they are authentic or not. Sparks discussion within the Literature Analysis.	Increased security and tamper-proofing				
39	Aamna Tariq et al. 's research article, "Cerberus: A	2019	**Indicating** global report statistics in 2013 that corruption within education is a worldwide issue. It is also more prominent within developing countries. Establishes current methods of	Increased security and tamper-proofing				

	Blockchain-Based Accreditation and Degree Verification System"		counterfeiting; Document fraud, Institutional fraud, Diploma Mills, Accreditation Fraud.					
40	Bhekabantu Ntshangase and Steven Msosa's research article, "The role of the South African qualifications authority in curbing misrepresentation of qualifications"	2022	Adding onto the list above: Translations.	Increased security and tamper-proofing				
41	Tasfia Rahman et al.'s research article, "Verifi-Chain: A Credentials Verifier using 50 Blockchain and IPFS"	2023	**Providing** evidence of multiple devoted fraudulent organizations that service and provide fake academic certificates to anyone who is willing to pay. Providing results that indicate it is extremely time consuming, taxing and simply difficult to authenticate genuine academic credentials. Clearly indicating that blockchain is the way of the future, but it also offers a case study tool for a peer-to-peer network protocol called "The InterPlanetary File System" (IFPS) with a clear explanation. Adds discussion within the Literature Analysis.	Increased security and tamper-proofing				
42	Seong-Kyu Kim's research article, "Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm"	2022	**Proposing** artificial intelligence to assist with digitization issues (that Rahman et al. presented). Indicating that institutions would have to invest large sums of money, time and resources into converting old credentials into digitized versions. Indicating an idea of marrying hash functions and artificial intelligence, as artificial intelligence helps with "selective management of necessary data" (Kim, 2022).		Streamlined verification process			
43	Joanna Black and Cody Fullerton's journal article, "Digital Deceit: Fake News, Artificial Intelligence, and	2022	Supports Seong-Kyu Kim's (2022) research article **Indicating** that educators must be made aware of disinformation and misinformation, as the internet offers a vast expanse of information and the vast progression of artificial intelligence, illegitimate research and current counterfeit methodologies. Sparks discussion within the Literature Analysis.			Changes in implementation	How blockchain technology may be used to introduce valuable	

	Censorship in Educational Research"						educational resources	
44	Aamna Tariq et al.'s research article, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System"	2019	**Indicating** that even developed countries serve as the largest markets supporting underground credential forgery markets. UK, US, China. Supporting research in credentialism, adds discussion within the Literature Analysis.			Changes in implementation		
45	Lonias Ndlovu and Andrew Leslie's research article, "False or Fake Qualifications in an Employment Context: A South African Perspective"	2022	**Indicating** that there is clear pressure for employment and/or promotion - for additional monetary bonuses. Due to this, it causes an overall rise in competition within the job market.			Changes in implementation		
46	Bhekabantu Ntshangase and Steven Msosa's research article, "The role of the South African qualifications authority in curbing misrepresentation of qualifications"	2022	**Indicating** statistics within South Africa that in six of the nine provinces, there is more than 50% of the employed that have a level of education below matriculation. According to Statistics South Africa's (2016) report, 58.8% of jobless individuals had less than a matriculation certificate, followed by 32.4% having a matriculation certificate			Changes in implementation		
47	Shivangi Dhawan's online research article, "Online Learning: A Panacea in the Time of COVID-19 Crisis"	2020	**Explaining** the changes institutions had to go due to COVID, as into the pedagogical approach of traditional face-to-face teaching and learning adapted into e-learning.			Changes in implementation	How blockchain technology may be used to introduce valuable educational resources	
48	Fawaz Habbal's journal article, "The	2023	**Indicating** that digitized, freely-available online research has necessitated technologies that have the ability to verify and give		Streamlined verification process	Changes in	How blockchain technology	

	Implications and Efficacy of Online Verification Tools inScientific Research and Citation Practices"		credibility to academic articles. Indicating the need and recommending future research for a sustainable, desired tool to monitor academic conduct.			implement ation	may be used to introduce valuable educational resources	
49	https://ucentralasia.org/schools/registrar/degree-verification	2025	**Case study examples**. They do not disclose how their blockchain database operates. Website and not a research article. Adds discussion within the Literature Analysis.		Streamlined verification process	Changes in implement ation	How blockchain technology may be used to introduce valuable educational resources	Present implemented blockchain resources
50	Elizabeth Durant and Alison Trachy's online article, "Digital Diploma debuts at MIT" https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017	2017	**Case study examples.** Introducing 'Blockcerts Wallet', explaining how their blockchain database operates within their institution in the form of a user-friendly application. Indicating that autonomy of student credentials allows the sharing of credentials without a concern of security risks. Adds discussion within the Literature Analysis.		Streamlined verification process		How blockchain technology may be used to introduce valuable educational resources	Present implemented blockchain resources
51	MIT's direct webpage article, "University of Melbourne to issue recipient-owned blockchain records" https://www.unimelb.edu.au/newsroom/news/2017/october/university-of-melbourne-to-issue-rec	2017	**Case study examples**. Indicating their collaborative use of 'Blockcerts Wallet'. Adding into the research findings that if an institution were to close down, the credentials will still be able to be verifiable on 'Blockcerts', the accredited third party.		Streamlined verification process		How blockchain technology may be used to introduce valuable educational resources	Present implemented blockchain resources

	ipient-owned-block chain-records							
52	The City University of Paris's website article, "Credentials on Blockchain" https://cityuparis.fr/credentials-on-blockchain/	2023	**Case study examples**. Indicating their use of a QR code where a graduate/student may direct users to a webpage for credential verifications. They do not disclose how their blockchain database operates, and only indicates the benefits of one.		Streamlined verification process		How blockchain technology may be used to introduce valuable educational resources	Present implemented blockchain resources
53	University of Johannesburg's website article, "UJ implements Blockchain-based Certificates for graduates" https://news.uj.ac.za/news/uj-implements-blockchain-based-certificates-for-graduates-2-2/	2022	**Case study examples**. Also indicating their use of a QR code with similar system dynamics to The City of Paris. Indicating that this university was the first in South Africa to implement a blockchain-based credential verification system.		Streamlined verification process		How blockchain technology may be used to introduce valuable educational resources	Present implemented blockchain resources
54	Abubakar Mohammed and Bashir Maina Saleh's journal article, "Centralised Database: A Prerequisite for Security and Sustainable Development in Nigeria"	2017	**Indicating** that a centralized database allows an authority to harmonize information within a singular data storage unit, delegating tasks to their respective administrative team and providing specific access to users in the database.		Streamlined verification process		How blockchain technology may be used to introduce valuable educational resources	
55	Aghayev et al. 's journal article, "Virtopsy – The concept of a	2008	**Indicating** a need for centralized databases to address vulnerabilities and opting for a standardized, digital documentation tool that may offer collaborative initiatives.		Streamlined verification process		How blockchain technology may be used to	

	centralised database in forensic medicine for analysis and comparison of radiological and autopsy data"						introduce valuable educational resources	
56	Joseph Enoch and Bourdillon Omijeh's research article, "Comparative Analysis of Blockchain and Database"	2023	**Giving** statistical data that indicates that researchers may only use approximately half of the capabilities of modern technology to apply to or enhance their research.			Changes in implementation	How blockchain technology may be used to introduce valuable educational resources	
57	Julian Springer and Philipp Haindl's research article, "'Blockchain-based PKI within a Corporate Organization: Advantages and Challenges"	2024	**Indicating** that DLTs have the option of cryptographic techniques and blockchain technology integrated with its systems. They indicate blockchain compatible with PKIs. Blockchain technologies are widely used due to their multiple points of failure, lack of central authority, and peer-to-peer environment; indicating blockchain technology's maturity, advanced security techniques and strong security.	Increased security and tamper-proofing	Streamlined verification process		How blockchain technology may be used to introduce valuable educational resources	
58	Bhabendu Mohanta et al's review article, "Blockchain technology: A survey on applications and security privacy Challenges"	2019	**Critical foundational theory**. Simply **indicating** that decentralized databases maintain a copy of ledger on a network of multiple nodes.	Increased security and tamper-proofing			How blockchain technology may be used to introduce valuable educational resources	
59	Siful Islam and Kutub Apu's research article, "Decentralized vs. Centralized database solutions in blockchain: advantages,	2024	**Indicating** that decentralized databases excel in enhanced security and transparency, particularly scalability and efficiency - especially in scaled environments with increased transactions.		Streamlined verification process		How blockchain technology may be used to introduce valuable educational resources	

	challenges, and use cases”							
60	Jesse Yli-Huumo et al.’s research article, “Where Is Current Research on Blockchain Technology?	2016	**Similarly indicating** that decentralized databases are a challenge in its widespread adoption due to poor scalability. Adding a practical example; as Bitcoin takes around 10 minutes to add a block to the chain.		Streamlined verification process			
61	Wang et al. 's research article, “vChain+: Optimizing Verifiable Blockchain Boolean Range Queries”	2022	**Indicating** simply that organizations that focus on data security and transparency will favour decentralized databases. However, centralized databases may be chosen due to greater efficiency (performance and scalability).		Streamlined verification process			
62	Yakubov et al.’s research article, “A Blockchain-Based PKI Management Framework”	2018	**Indicating** a workaround to blockchain scalability issues, as the marriage of PKI and blockchain technology produced pleasing and acceptable maintenance costs, as well as speedy performance and transaction rates.		Streamlined verification process			
63	Qurotul Aini et al. ‘s research article, “Blockchain Based Certificate Verification System Management”	2022	**Indicating** that certificate revocation management has worsened due to cloud computing and The Internet of Things (IOT). IOTs have many vulnerabilities due to openness and connection of use cases. Therefore, cryptographic solutions (blockchain technologies) may resolve some of these issues with strategies.		Streamlined verification process	Changes in implementation	How blockchain technology may be used to introduce valuable educational resources	

4.2 Literature Analysis

Literature Analysis has been organised according to the detailed core research questions found in the Introduction. The purpose of this section is to go beyond systematic paraphrased summaries, engaging in a hybrid of critical analysis and discussion within the South African context.

4.2.1 Research Question 1

How can unique blockchain encryption technology be used to secure and validate higher education institutional product outputs (diplomas, degrees, and certificates) to fight counterfeiting, and what resources would it cost to implement and maintain such technology?

4.2.1.1 How can blockchain technology be used to secure and validate higher education institutional product outputs (diplomas, degrees, and certificates) to fight counterfeiting?

Uniqueness within Limitation

In the thesis's limitations, it was made clear that a Masters level thesis was not able to go through as thoroughly as desired due to the scope and limited capacity of research. In additional reasoning, there was a large limitation due to the **lack** of prior deep knowledge within the field and understanding of algebraic mathematics that could not be applied to the paper. Optimistically, this gives clear opportunity for future research and provides a possible supporting stepping stone. Additionally, the thesis is aimed to give a deeper understanding that places blockchain technology in various contexts **outside** of NFTs and cryptocurrency. It may be argued that the researcher may give valuable insight as someone who had **no** prior in-depth knowledge on the subject. Presenting reasoning and argument; if institutions and organizations are to implement blockchain technology within their systems, how would it affect the cost of resources to implement and maintain such technology? Cost may not mean monetary in this context, as it is more prevalent in a **focus of knowledge**. How long would an average working individual come to understand the inner workings of a new technology within their older systems? The thesis itself is a valuable (**and unintentional**)

experiment to this question, as it is written from the perspective of someone that had no prior deep knowledge on cybersecurity.

This thesis has **no scope** for suggesting an optimal system for a blockchain-based database within South Africa, and especially for the University of the Witwatersrand. It is within a **self-argument** and **limitation** that suggestion and theorisation of an innovative technology are insufficient without a prototype and test data. Witnessed research that proposes implementation of blockchain technology all similarly have **customized blueprints** with **quantitative results**.

However, it is beneficial for the thesis to conduct thorough qualitative research, so that it may **start a conversation**, expose critical information and research gaps, and reveal the differences and intricacies of an innovative technology. The thesis, thus, intends to not put an actual blockchain system together, however only provide a stepping stone and prompt it in the right direction.

In support of this thesis that touches enough on the basics to project forward into more complicated contextualization, Johnathan Bevers's (2021) thesis, they explain complicated asymmetric algorithms used in blockchain technology **comprehensively** and **simply**. The **format** and **simplicity** of the author's thesis is commendable, compared to the lack of this trait when researching this particular subject. This shows a clear research gap, as the amount of extensive algebraic research papers observed were **immensely complicated** and **overwhelming** as a researcher that is not completely familiar with such advanced technologies at the time. Additionally, this may not be appropriate for a researcher without a mathematical background. There is the same observation made by Bevers, **and** in Shuyi Pu and Jasmine Siu Lee Lam's (2023) research article, validating the initial expression of this thesis where it is indicated that there is a **need** for new technology to be broken down into easy, digestible pieces if we want it to be introduced into society as a foundational norm.

Credentialism

(*reiterate research problem*) Focusing on the core research question, in identifying the socio-economic causes of digital counterfeiting proved an **exceptionally** important sub-research question, as it prompted the rise of ***understudied phenomena***. Originally, personal researcher assumptions were that it would address South Africa's prevalent poverty, crime and quality of life difficulties as a reason for degree counterfeiting. However, it suddenly delved into great detail with

unconsidered and unexpected concepts. According to Lonias Ndlovu and Andrew Leslie's (2022) research article, they **do** indicate poverty to be a source of reason when there is extreme competition within the job market in South Africa. However, Aamna Tariq et al. 's (2019) research article alternatively indicates that even **developed** countries statistically show a **higher** demand for underground markets for fraudulent practices. This is all due to the contribution of problematic **culture**, rather than simply labelling it as 'poverty'. There is evidence supporting the increase of competition within the job market, as well as an **over-reliance** on credentials even for moderate to low skill positions. It is believed that competence within the workplace is **dependent** on the institutional qualifications of the applicant, using it as an indicator for dependability, talent and work ethic.

In Dictionary.com's (2025) definition of counterfeit, it is the **intention** of deception in the **illusion** of something genuine. In the research, it is found that the scope of counterfeit is **not** just credentials (even though there was a hyperfocus on validation of degrees, certificates and diplomas), but resulted in a variety of actions within an education institution. Findings suggest through conclusive observation that credential counterfeit is only a **broad** segment of **many** problems higher education institutions are faced with.

Ultimately, humans pursue and acquire credentials for a purpose, primarily employability within a professional field of personal interest and choice. Therefore, the term "**credentialism**" has sprung up with further research. Mentioned in Aamna Tariq et al. 's (2019) research article, Lonias Ndlovu and Andrew Leslie's (2022) research article, as well as Lisa Guernsey's (1997) article, "Is the Internet Becoming a Bonanza for Diploma Mills?", they all introduce and discuss the **negative** impact of **extreme** credentialism. It is important that Lisa Guernsey's (**1997**) article was mentioned in this piece, as it is an indicator that it had always been an **ongoing issue** in its comparative evidence of the year all articles were published. It can be argued that digitization of physical credentials, the explosion of highly advanced **counterfeit-enabling** technologies and the entry into the 4th industrial revolution had **worsened** credentialism.

Additionally, Lisa Guernsey's (1997) article explains an extremely valid point; the unjust denial of people who do not have the adequate qualifications for a job application or **promotion** is enough reason for people to intentionally acquire counterfeit qualifications. As an employer depending on university qualifications to estimate work eligibility, this becomes a double-edged sword. If we had to argue and give an example of an employer refusing a job applicant for a medium or low skill

position due to lack of university qualification, would that job be significant enough to cause noticeable damage within the sectors of the economy? Obtaining fraudulent credentials to combat credentialism may **seem** justified, however, it is **still illegal** and extends out to organizations who may not indulge in this approach - such as the example of university lecturers applying for jobs to teach with fraudulent qualifications.

While blockchain technology may not be able to address the negative impacts of **credentialism,** it does have the ability to **completely eliminate** counterfeiting techniques, criminal groups, major profitable underground organizations and black markets. It offers a form of trusted regulation, and prevention of tragic criminal cases, such as the murder of an Unizulu professor in The University of Zululand. In Karabo Ledwaba's (2018) online news article, "Unizulu professor killed over fraudulent PhDs", the university had been facing a credential fraudulence crisis and the victim had been actively working against counterfeit PhD's. However, it is alleged that due to the victim's prior filing of an intimidation charge against threats from a colleague that was caught with a fraudulent PhD, the murder had been intentionally premeditated and targeted. Therefore, with the introduction of blockchain technology and the ability to authorize the credibility of PhD's, it is with trust that it may prevent incredibly sad situations like this.

Blockchain Technology: An Adaptable, Scalable and Flexible Security Technology

Blockchain makes use of cryptographic, mathematical algorithms to ensure privacy, integrity of data, entity authentication, and data origin authentication, according to Mathe et al. 's journal article. Upon further investigation, blockchain is only a product of security science and utilizes cryptographic techniques to run specialized, customized and detailed algorithms. It is important to note, in terms of research findings, that the thesis will be unable to thoroughly discuss a wide range of algorithms within its scope.

Therefore, in respect to a deductive methodology approach, this section will begin with a broad introduction of an existing theory and narrow into a detailed collection of data to answer the core research questions. Therefore, to **thoroughly** understand how unique blockchain technology may be used to secure and validate higher education institutional product outputs (diplomas, degrees, and certificates) to fight counterfeiting, it is extremely beneficial for the literature review to outline core definitions. These definitions will not be repeated here, however, only **major findings** will be indicated and analyzed.

There is evidence that hash functions have proven to be an extremely useful tool within security science, as Rajeev Sobti and Geetha Ganesan's (2012) journal article builds upon Praveen Gauravaram's (2003) thesis. Conclusively, this indicates the longevity of the digital security tool. In research findings, this is due to the practical ability for hash functions to **be customizable** and **evolve** according to the progression of digitization and algorithms. Both Rajeev Sobti and Geetha Ganesan's (2012) journal article and in Qing Zhou et al.'s (2023) research article indicate similar findings were hash functions that "***digital identification, message authentication, digital signatures and pseudorandom number generation***" within a modern society and its available and **expanding** digitized services (Qing Zhou et al., 2023). With an array of uses for hash functions, Shashwat Sharma and Ayush Mishra's (2024) research article further reiterates that the process is **trustless**, **immutable**, **automatic** and **secure**, as there is therefore **no central authority**. This is supported by Marut Pandya's (2024) research article.

Interestingly, in Qing Zhou et al. 's (2023) research article, they introduce **quantum-based hash functions**, which ultimately indicated that hash functions **afford a variety** of hash functions developed according to a variety of distinctive needs of the organization. In further study, it was noted that there are **classes** of hash functions. Blockchain technology is well known to use SHA-256, which translates into a **S**ecure **H**ash **A**lgorithm. If an education institution would choose a hash function, it is important to understand that older models (such as MDA or SHA-1) must be warned of the potential of it growing obsolete and its susceptibility to collision attacks. However, SHA-3 is intended for extremely high security systems with a need for additional cryptographic strength. A newer model will always begin to outdate its predecessor, especially the mention of quantum computing in Deepanshu Rana's (2024) journal article. With the introduction of quantum computers, blockchain solutions **may promise to** prevent potential problems in the future against **progressive** and **aggressive** technologies if implemented **now.**

If hash functions are implemented into an education institution, they serve as a **record** on the **blockchain**.

Table 3

An example of a hash function.

The input variable, let's say for example, "Bob made donuts", is converted through a SHA-256 hash function algorithm to produce a fixed-output length: (*hash value = 8a19ec975c9568e3fa064a14c14fad200d2a611ffa113c3945098889c62c4f89*). If there had to be a **typo**, "Bob made *domuts*"; (*hash value = dde2cf25812b13fd3c036737ab6066b082d97dff9c070078715b83723f1edb0a*). SHA-256 generator: https://emn178.github.io/online-tools/sha512_256.html

This is a relatively simple algorithm with a simple concept, however, it may be applied to many functions within a system. Therefore, if hash functions are implemented into a higher education system within South Africa, its main purpose would be to **ensure that records have not been altered**. If this can be put into a contextual example;

An input variable that is converted through a SHA-256 hash function algorithm produces a fixed-output length. The fixed-output length is encrypted with a key (asymmetric or symmetric, depending on the needs of the organization). It is then recorded on the blockchain. Therefore, it may be used as a form of a **digital signature,** allowing for many uses within a higher education institution;

- Mainly, for digital certificates (***credentials***) to be authorized and authenticated through the institution and stored on their blockchain database.
- Secondly, for electronic signatures of administrative documentation, such as authenticating legitimate staff contracts from Human Resources (from the correct people), as well as any official communication from the higher education institution. This can also, logically and simultaneously, reduce **phishing**.
- Thirdly, hash function outputs and digital data that are recorded on the blockchain have **multiple points of failure**. Therefore, it may be easily recovered, unlike a single point of failure. Additionally, it increases **accessibility** through the flexibility and convenience of

online administration. It is easy to argue and say that a modernized, flexible and smart digital database is extremely appealing in comparison to a physical paper database.

- Fourthly, a digital signature may **streamline multiple modes of administrative tasks**. It may range from departments, such as Human Resources, all the way to the lecturer that may authorize their gradings and official communications. Giving digital signatures to students may possibly also allow the student to authenticate the identity of their work in given contexts (such as significant research within a Masters or PhD paper), as it may provide clear ownership to the researcher through the records within an institutional blockchain database if the paper is compromised. In addition, it can offer the service of an indication of legitimate attendance in compulsory lecture/seminar sessions.

In the proposition of an idea, perhaps a physical fingerprint of a human could be tied to a digital signature as a progressive result of the evolution and marrying of **digitization** in a **physical** space. If a physical fingerprint is already being used at The University of the Witwatersrand, as an example, to authenticate identity at **turnstile gates**, it indicates that there is an active profile of that person on a database. If that physical fingerprint was recorded as a digital signature, and the database had blockchain technology to accommodate it, how far would the digital database be utilized if it is recorded on the blockchain through an **automated** algorithm? This pushes the idea of digital signatures going beyond a purely digital dimension, making a human's own fingerprint a digital signature that is recognized within their physical facility and reflected in digital systems. In supporting theory, it naturally **automates administration** and **record keeping**, and guarantees immutability; however, **it tracks movement** and may cause privacy issues if implemented incorrectly. If this does inspire future research, it is extremely important to note that it is a **main priority** to ensure that all technologies are used responsibly, reasonably justifiable and ethically.

As a further additional point and general observation, smartphone functionality of being able to unlock it with a fingerprint has now been integrated with Google - as now the user may enable two-step verification using their own fingerprint to secure their email login. If this technology is pushed into the daily life of a student, lecturer, or administrative staff, this may offer an enhancement to quality of life and legitimate digital presence.

The theorization above may be a stretch, an outlandish approach to suggest a complete innovative digital overhaul of education institutions, however it is hoped that maybe in a few hundred years time, this might not be such a foreign concept after all.

Therefore, in fundamental literary evidence, this information is also supported of both Shashwat Sharma and Ayush Mishra's (2024) research article and Marut Pandya's (2024) research article indicate that the hash function operates automatically (the use of an **engineered algorithm** that automatically records on the blockchain), trustless and secure (non-dependant on human labour). No **random** person will be able to decipher the input variable, however the *hash value* is **fixed** on the blockchain. Taking away from their research article, the main finding is that SHA-256 is primarily used in blockchain technology due to the balances between **performance** and **security** in comparison to other hash functions. In Guangyuan Chen's (2024) research article, they introduce three cryptographic algorithms used for creating digital signatures. Narrowing down from blockchain technology, into cryptography, into hash functions and now digital signatures. Digital signatures prove **authentication,** integrity and prevention of repudiation. A blockchain system within a higher education institution may want to consider the use of digital signatures in order to digitise a fingerprint and verify the user.

Critically, in Guangyuan Chen's (2024) research article, they investigated further into **ECDSA** (Elliptic Curve Digital Signature Algorithms) and primarily conducted research addressing **privacy** concerns. Blockchain technology is characteristically transparent when transactions are recorded, and therefore, Chen (2024) proposes **zero-knowledge proofs** and **homomorphic encryption**. This is further supported by Liz George and Jubilant Kizhakkethottam's (2021) research article, where these above two were the **most major solutions** to external organizations within the supply chain opting for blockchain technology and demanding privacy and confidentiality. Contextually, in higher education institutions, **zero-knowledge proof** would be optimal for record of transactions while hiding selected sensitive information - such as (*in theory*) verification of credentials and smart contracts (administrative tasks). Homomorphic encryption may also be used in handling data within its encrypted ciphertext without it being decrypted, retaining privacy through its handling (Liz George and Jubilant Kizhakkethottam, 2021). Therefore, this (*in theory*) could be private communication with the university and the student.

Additionally, a blockchain system within a higher education may find the situation where credentials may need to be **revoked** due to a case of academic misconduct (graduates who are caught with plagiarism etc.). It is argued that it is **also** a lack of academic integrity if it was impossible to revoke credentials for any valid reasoning. According to Aamna Tariq, Hina Binte Haq and Syed Taha Ali's (2019) research article, they developed a blockchain technology solution called **'*Cerberus*'** with an **'*on-chain credential revocation mechanism*'**, a **declaration** of revocation using an '***Implementation Engine***'. It is with clear evidence that blockchain technology and cryptographic techniques may address problems and offer solutions through dedicated and focused research groups.

Standardization, One Size Fits All?

Interestingly, Deepanshu Rana's (2024) journal article suggests a point of **standardization** if a blockchain solution was proposed to multiple education institutions. In the article above, it said that institutions would need to engage in **mass teamwork** for this to happen. This brings up the discussion of the same concept applied within the thesis question (*how blockchain technology can be used in the context of South African higher education institutions*), the same idea that was brought up earlier in regards to setting a framework and standardization within South Africa, mentioned in the Literature Review. Particularly with regards to the Dineo A. Matlebjane and Patrick Ndayizigamiye's (2022) research article indicates that there is not even an established, standardized framework with a normal collective centralized database for healthcare patients within South Africa. This prompts the point that standardization is an extremely **arguable** and **complicated** concept for higher education institutions. Firstly, it is understandable that having a standardised framework may enable technological enhancement.

In a critical additional note that supports the above argument, Elizabeth Durant and Alison Trachy's (2017) online article in association with Massachusetts Institute of Technology (**MIT**) had indicated their utilization with an application called **'*Blockcerts Wallet*'**, developed in collaboration with Learning Machine and their internal MIT Registrar's Office. They offer an incredibly resourceful argument to the thesis, highlighting their **'*Blockcerts*'** application that had **also** been utilized by The University of Melbourne. **Standardization** may be possible if blockchain based databases are engineered and then licensed and offered as an **open-source code**. A higher education institution, especially in the context of South Africa, may consider utilizing this as well. A link has been provided below for any potential further research.

https://www.blockcerts.org/guide/faq.html

However, it is arguable that higher education institutions operate on their own, and indulge in **their own** databases. Each organization has distinctive needs, including the scale of their administration, students and staff. While it is useful to produce open-source papers that indicate how to use blockchain technology within an institution, like Awatef Balobaid et al. 's (2023) research article, “Modeling of blockchain with encryption based secure education record management system” as a prime example, there is need for further consideration. As in Guangyuan Chen’s (2024) research article, they discuss a **‘post-quantum cryptographic algorithm’** that meets certain criteria for certain protocols in their research. Therefore, this indicates that there are **multiple, and symbiotic** methods of implementing hash functions, digital signatures and cryptographic security options into a system, making it glaringly obvious that there is **not a linear** way of ensuring an effective implementation of blockchain technology without considering the needs of the system.

Blockchain technology is not bound to SHA-256, and may host a multitude of different hash functions as well as blockchain protocol. The hashing algorithm that a cryptocurrency uses has a significant impact on its security, scalability and energy efficiency. From the findings, it indicates that SHA-256 is an effectively secure hashing algorithm, however it is also **energy-intensive**. Therefore, some cryptocurrencies have opted for different hashing algorithms that are more scalable and energy-efficient. Interesting and importantly, a general observation from research papers that discuss **how** to implement blockchain into an education system have all **built their own**, tailoring it to specific needs of their institution and suggesting it as a framework of operation. Evidence includes Shuyi Pu and Jasmine Siu Lee Lam’s (2023) research article and “***Blockcerts***”, or Awatef Balobaid et al. 's (2023) research article, their developed framework using a “***hash-function Merkle tree”,*** or Tasfia Rahman et al.’s (2023) research article where they introduce their peer-to-peer blockchain model "The InterPlanetary File System" (**IFPS**), or Aamna Tariq, Hina Binte Haq and Syed Taha Ali’s (2019) research article with the introduction of **“*Cerberus*”**. They also add a few more frameworks such as Turkanović *et al.* 's (2017) “***EduCTX***”. It is therefore **true** that there is **no standardization** in Deepanshu Rana’s (2024) journal article. It is therefore **understandable** to opt for standardization and collective efforts to implement a foundational system, **however** it conclusively results in a discourse with lack of research, data and institutional interest to fully answer this question.

However, taking a step back to see the bigger picture, it **does** *ironically* give a sort of **standardized framework in its own way**. All research articles indicate a certain criteria to create a blockchain-based system for higher education institutions based on these observed recurring factors;

- **Scale** of the institution (amount of students, staff, academic influence and generation of research articles, research availability, funding into technological upgrades, funding into training staff to understand technological upgrades).
- **Critical needs** of the institution (assessment of current problems - such as the example of The University of Zululand and its fraudulent credential crisis).

Which Key for What Purpose?

In reiteration, it is clear from the above paragraphs of the chapter that each organization is **customized** to its needs. From Chapter 2: Literature Review, it elaborates the fundamental details within Symmetric (Private) Algorithms/Keys and Asymmetric (Public) Algorithms/Keys. When applying this information to the core research question, "*How can blockchain technology be used to secure and validate higher education institutional product outputs (diplomas, degrees, and certificates) to fight counterfeiting*?", it is clear that both public and private keys may work **symbiotically** within a blockchain-integrated system for different roles. It is **difficult** to answer this question bluntly, due to a range of complex, custom models that may be implemented into a blockchain database.

Therefore, Hind Alshambri and Fawaz Alassery's (2021) research article, "Securing Fog Computing For E-Learning System Using Integration of Two Encryption Algorithms" assists with answering this question in a more simpler way with an example. They utilize **I**ntegrated **E**ncryption **S**chemes (**IES**), a **hybrid** model using **both symmetric** and **asymmetric keys**. Within their utilization of blockchain encryption technology to enhance security in e-learning, their results indicate;

the use of authentication- a public key encrypting a symmetric key, identifying and verifying the sole viewer of a file.
the use of authorization - only a system administrator gives the student their private key to read files only.
the use of confidentiality - using a combination of AES and RSA encryption, files are encrypted until they are delivered to the intended receiver.

the use of integrity - using a one-way hash function, such as MD5 (**an older model**), which ensures record transmutability of any 'transaction'.
In their conclusion, they indicate that algorithms are chosen according to hardware and system requirements. Algorithms such as RSA, AES, and ECC results in being evidently **sustainable**.

Additionally, according to Seied veria Hosein's (2018) thesis, "Mathematics and Data Structures in Blockchain and Ethereum", it touches back onto public and private Blockchains. Approach recommendations for the education sector are entirely case-specific, however **hybridisation** may be the most appealing option. Private blockchains are considered ideal for storing internal student smart contracts (which may contain sensitive information); the network requires authentication and consensus authority for access (Hosein, 2018). Additionally, the characteristics of a private Blockchain allow for privacy and authentication of assorted, controlled administrative workflows within an education institution. In addition to an operating **private** Blockchain within the institution, a **public** Blockchain may allow for a trustless verification of credentials from external users (people outside of the institution that may want to verify an employee's credentials) - a major and simple solution for fraud prevention - by publishing unique hashes on the blockchain, which represents intangible evidence of the credential/achievement within an institution.

Therefore, in critical discussion of this particularly difficult section, it is recommended that in order to determine system requirements and hardware specifications, **quantitative research** must be conducted **internally** within the university/organization. Suggestions include conducting interviews and handing out surveys on staff members (administrative roles and lecturers) to identify key system unproductivity (inconveniences that may hinder work productivity). This may branch out to the rest of the university/organization; assessing interviews and handing out surveys on students. Additionally, as said before, but to identify any **ongoing problematic crisis** (such as fraudulence and credential-counterfeiting epidemics).

The Role of Steganography

While it may be odd to include steganography in a thesis that harps on cryptography, research findings indicate that within its **cousin** (Haque et al., 2020), **steganographic** information adds an **insightful addition** to the usage of blockchain technology within a higher education institution. The evolution from web2 to web3 had forced the emergence of a digital age, where physical steganographic forms of security are **not** often used anymore due to its natural depletion into

obsoletion. With the emergence of modern digitization, there is a forcible shift from the physical to the digital realm and therefore all organizations are **compelled** (due to criminal activity and security compromisations) to implement new techniques to authorise digital documentation. Therefore, with the assistance of digitization and artificial intelligence, it is far easier to generate imitative counterfeit documentation. Reiterating and reinforcing this concept, as Edward Lucas says, "***A cover identity that would have been almost bulletproof only 20 years ago can now be unravelled in a few minutes***" (Lucas, 2019). Technology has progressed so far, and time will tell when any technique becomes obsolete or not. This is true when looking at SHA-1 compared to SHA-3, and eventually into inevitable quantum computing algorithms in the future. The research's findings were originally intended to demonstrate how much more **secure** it is for educational institutions to **just** use blockchain technology to reinforce their databases and information, however it is now seen as an **opportunity** for growth and progression in our history and time. There is much more to it, and security is only one minor advantage to the overall concept.

However, according to Seong-Kyu Kim's (2022) research article and Joanna Black and Cody Fullerton's (2020) research article, they **strongly** indicate that there **cannot be a regression of time** back to old methods of document authentication (steganographic techniques).

Additionally, according to Haque et al. 's (2020) research article, steganography is only **part** of a broader concept that offers **multiple** forms of protecting and hiding data as a **whole**. As mentioned as a key result of the paper, there is a proposition that there could be a **harmonious** union between **all** forms of authentication, as they all serve their particular functions within the institution. Although blockchain technology does **not** include steganography, it may be argued that it is still important to include both cryptographic and steganographic techniques within a higher education institution. The main **argument** proposed in this section is to question the **implementation** of blockchain technology within a higher education institution. To put it simply, Rome was not built in a day, and having both techniques may serve to **bridge the gap** from the physical to the digital; or potentially even having both. *This is the opportunity for growth and progression in our history and time.*

Steganographic techniques such as holograms on physical banknotes are **still** used, and have maintained their legitimacy **despite** modern digitization techniques within the 21st century. Therefore, degrees, diplomas, or certificates in its physical form may also have some form of

physical authentication. It may be argued that credentials are **not standardized** like bank notes are, and therefore physical authentication may be absent.

Additionally, according to Mohammad AlKhanafseh and Ola Surakh's research article, "A New Evidence Preservation Forensics Model Using Blockchain and Stenography Techniques", they discuss the use of steganographic techniques within blockchain models in the context of preserving forensics and evidence within a database. These steganographic techniques discussed in the above research article include '***the first level involves dividing evidence into chunks, resulting in a higher level of complexity. The second level involves distributing the chunks over blocks of equal size, embedding the chunks using steganography and blockchain technology*** (AlKhanafseh and Surakh, 2024). However, further research must be conducted to determine the system strain, cost of maintenance (electricity and possible troubleshooting).

Conclusively, while steganography may serve as a **weaker** argument compared to all other points within the *Literature Analysis* section, it may serve as a humble reminder that a complete overhaul is impossible overnight. Additionally, due to research found that unified steganography and cryptography techniques adds an additional layer of security to institutions that may be handling sensitive information.

However, **before** improving organisational quality of life, blockchain technology may begin to address **urgent and critical concerns** like counterfeit and student **credential validation databases**. In terms of thesis awareness and introspection, the core research question was originally a response to major credential counterfeit problems within South Africa, as well as internationally.

4.2.1.1 What resources would it cost to implement and maintain such technology?

Artificial Intelligence and Blockchain

The theory of *understudied phenomena* has proven itself; *how new academic research and writings on innovative technologies must be conscious of* ***unexpected results from theoretical ideas*** *(p.15).* Putting

this theory into practice, and gradually conducting research for the thesis, several **notable** ideas and **keywords** have emerged.

While this thesis is framed within the context of South African higher education institutions, the research question is more applicable and universal. As mentioned in the *Chapter 1: Introduction* (*p. 5*) section of this paper, "*Blockchain technology in itself has notably been severely overlooked by educational institutions and society, thus opening an overwhelmingly vast expanse of potential research opportunities in its positive impact on daily life*", this statement has been proved to be verifiable due to the conducted research. The emergence of an equally-rampaging and rapidly-growing technology, **artificial intelligence**, has posed significant challenges. According to Seong-Kyu Kim's (2022) research article, they interestingly propose **using** artificial intelligence to **assist** with **digitization issues** that Rahman et al. (2023) presented in their research article. Seong-Kyu Kim's (2022) indicates that institutions would have to **invest** a large sum of **money**, **time** and **resources** (labour-intensive) into converting old, physical credentials of past students into digitized versions. Akinradewo et al. 's (2022) research article indicates the same issues, with the addition that it may be extremely time consuming to implement updated and reiterated systems, however it is within the context and **boundaries** within South Africa. Furthermore, both research articles mention that there would be funds needed to train or hire staff members to ensure an adequate workforce.

However, in direct argument to this, quantitative research had been carried out in Bakri Awaji and Ellis Solaiman's (2022) research article, "Design, Implementation, and Evaluation of Blockchain-Based Trusted Achievement Record System for Students in Higher Education", in order to determine how students and staff members would react to an updated, prototype blockchain database system. **Critically**, it was found that with a blockchain database designed to be user friendly, users strongly **disagreed** with the statement that they had to learn a lot of things before using the updated system. It had also been indicated that "***43.33% of participants strongly disagreed and 30% disagreed when asked if the system was complex***" (Bakri Awaji and Ellis Solaiman, 2022). They also expressed that skilled expertise and training was **not** needed to operate it efficiently and confidently.

Therefore, it is clear with the above research articles that training staff and students to use an updated and reiterated system will **not** be an issue if the system is engineered and designed with user-friendly accessibility in mind. **Artificial intelligence may assist with extreme labour-intensive tasks** (such as inputting and converting past-graduate credentials into the new blockchain system).

However, it may be argued that engineering and **implementation** of blockchain technology is the most resource-intensive part of system reiteration.

Broader Implications of Findings

Broader implications of findings extends and applies to healthcare and public governance, such as the mentioned local example of the National Department of Health (2012) in their journal, "National Digital Health Strategy for South Africa, 2019 - 2024", which seeks to develop and provide a national, digital platform for storing healthcare data on patients, medicine, and human resources. Trust and integrity is vital, **especially with sensitive information on broader adoptions of the technology**. Therefore, in Siful Islam and Kutub Apu's (2024) research article, they propose a similar idea to this thesis - a blockchain solution which privatizes and centralizes control. Therefore, a **hybrid database model**. While it is clear through research findings that blockchain technology may be integrated according to specific needs of a database, it may extend out into **interrelated smart devices** (**IOTS**).

In an interesting addition to the thesis, blockchain technology and cryptographic techniques may offer an additional enhancement to **IOTs**, which are already aimed at enhancing the quality of life for humanity (personally or professionally), as defined by Kinza Yasar and Alexander Gillis's (2024) online website. With Qurotul Aini et al. 's (2022) research article in mind, they particularly indicate that there are many **vulnerabilities** due to **openness** and **connection** of use cases within the network or cloud it is connected to. They determine that cryptographic solutions (and blockchain technology) may resolve some issues. **IOTs** were actually mentioned in the previous paragraphs as the turnstiles at the gates within the University of the Witwatersrand, as well as the proposed automated biometrics that scan fingerprints and authenticate the user. It was suggested in the thesis that digital signatures may offer an enhanced security, streamlined automation and peace of mind within immutability.

However, this perspective may be extended due to **IOTs** that are factually integrated with many external professions and industries outside of higher education institutions. In a critical example, this may be in the form of prevention of tampering with malicious **aviation attacks**. According to Rashi Kaushik and Amit Thakur's (2022) research article, "A Brief Review on IoT, its Applications, Challenges & Future Aspects in Aviation Industry", they indicate that IOTs are used in flight communication, flight tracking and various management services, aircraft health monitoring and navigations. The researchers also indicate **critical cyber-security concerns** and terrorist attacks

and digital hijacking due to **IOTs** vulnerabilities. **It is worthwhile** to suggest blockchain technology as a possible solution to address these vulnerabilities. According to Razan Alajlan, Norah Alhumam and Mounir Frikha's (2023) research article, "Cybersecurity for Blockchain-Based IoT Systems: A Review", they assist in describing how blockchain technology may **decrease the risk of cybersecurity attacks** in the context of **IOT** usage;

- a decentralized technology may be difficult for an attacker to target due to the data being stored on multiple nodes,
- attackers may find it difficult to manipulate a blockchain-based system due to the nature of the algorithms (consensus mechanisms), where specific network participants are all required to agree to the validity of a transaction,
- encrypted cryptographic techniques will make it difficult for an unauthorized attacker to read,

It may be argued that the above information is devoid of the core research questions presented within the thesis, however, it is **within an ethical judgment and moral obligation** that the points made here are justified and extremely important; with the research findings of blockchain technology, evidence throughout the *Literature Analysis* indicate that it may pose significant aid in saving lives **within** the core research questions, and **within** the broad implications of its findings.

4.2.2 Research Question 2

How can blockchain technology be used to introduce valuable educational resources, such as decentralised, open-sourced data centres; what would their benefits and drawbacks be as opposed to current-day existing resources?

Unexpected Limitations

As the thesis conducted research within the *Literature Review* section, it was found that Research Question 2 had **already been half answered** in the Security and Validity section. Additionally, original research questions (*such as the example of if current blockchain-infused institutions are successful*) could not be answered due to the need for quantitative data and dedicated, independent investigations which needed the assistance of human interaction and **opinion**. However, it was not entirely removed from the thesis because it may have the potential to advance the research at a later date. It also simultaneously indicates a research gap, highlighting that while blockchain technology is being infused with higher education institutions, there is a lack of data on the outcome, results and user reaction.

Additionally, research discovered that it was also slightly more difficult to find information on various uses of blockchain technology, other than the discovered spotlight, which is credential verification within a higher education institution. However, the section still proved itself useful to push academic boundaries and indicate evidence that there may be **more than one utilization** of blockchain technology within a higher education institution. Additionally, it is useful to include the argument that credentialism and the need for additional security is seen as a **higher priority** than other uses for blockchain technology due to the ongoing negative effects of fraud and counterfeit degrees in academia. While it may be argued that Research Question 1 has stronger arguments, it may be also valuable to indicate a broader exploration of research that may be less prioritized but be considered at a later time. The thesis also affords this bit of extra scope.

Therefore, major findings within the literature indicated an introduction that blockchain technology to be a useful potential within **education institutions**. In Guang Chen, Bing Xu, Manli Lu & Nian-Shing Chen's (2018) article, they describe the utilization of blockchain technology to additionally **enhance the online learning experience**, such as a student achievement validation database, the use of digital currency as a form of student credit, and the concept of an automated smart contract that ensures consistent, high-quality work output. According to Shivangi Dhawan's (2020) online research article, they indicate that COVID-19 was a critical boost into the demand and adaptation of e-learning, from the pedagogical approach of face-to-face teaching and learning. However, it may be argued that COVID-19 was only **a forceful push** into an initially *gradual* evolution of technology.

Importantly, according to Fawaz Habbal's (2023) journal article, there is an indicated need for a modern, **digital tool** that **monitors academic conduct** and is **sustainable in the long-term**, having

desired characteristics such as ensuring "*scientific integrity, research productivity and scientific literature*" (Habbal, 2023). Additionally, Joseph Enoch and Bourdillon Omijeh's (2023) research article indicates that most researchers only utilize **half** of the true capabilities of modern technology (the emergence of an international and unlimited **digitized** online library) to tackle a research question as a result of a **higher quality of research**. However, in a broader perspective within the emergence of **AI** within our current-day existing resources, as seen from counterfeited credentials, this may **extend** further into counterfeit research articles, fraudulent references and artificially generated scientific literature. **Problematic** and **ethical considerations** may be questioned in response to this, as according to *Cambridge's* (2025) online definition of '*Artificial Intelligence*', indicates simply that it is a human-brain based machine that learns from **given data**. This data may be pulled from online open-sourced research databases, and may disregard and not give appropriate references to the respective researchers who had established the first foundational theories and frameworks, or have contributed to the growth within an academic field. The thesis offers blockchain technology as a sustainable digital tool that may monitor academic conduct, as in *Research Question 1 Results section* proved that blockchain technology may offer graduates to share their credentials without the concern of security risks. This concept may also, logically, apply to a researcher and their published research articles - especially those who offer it as an open-source material. While it may **not completely eliminate** the practice of academic misconduct, it is worth consideration as an enhancement to our current systems and educational resources within higher education institutions.

Sharing of Sensitive Information on Research 'Standardised, Framework' Databases

While it is unclear to determine the common type of database technology a higher education institution may use (due to obvious suspicions of prying, as well as the lack of scope within the thesis), the thesis may rather offer findings that are situational, offering the concept of, (in lack of a better phrasing), '*if an institution were to use this type of technology, they would...*' It is the recommendation that an institution may utilize the research, internalise it within their own context and potentially deliver a reformed system with these findings in mind.

Therefore, in research findings conducted through the *Literature Review*, a centralized database is one centralized authority with a dedicated administrative team, according to Mohammed and Saleh's (2017) research article. If a higher education institution were to implement a centralized database to function within, there is **limited access to specific information for the user base**. In the context of

research storage, in Enoch and Omijeh's (2023) research article, they indicate a wealth of information adds to a potential opportunity of misuse. Therefore, the main concerns of a centralized database is that it was **prone** to a **lack of regulation** and **misuse of technology** by the delegation of management within the employers, employees, users, or the institution. A centralized database relies on a standalone network, therefore a vulnerable, single point of failure. According to Aghayev et al. 's (2008) research article, they add on the point that there needs to be a certain amount of anonymity within the limitations of ethical information management. Interestingly, they use a very valid case study when **medical research** is uploaded into a database. It is expected that real medical cases abide by consent and ethical practices of both the sensitive information of the participant and the responsibility of the research institution. It is therefore that, after the research conducted through Research Question 1, blockchain technology infused with a digital database focused on providing educational resources may offer a way to navigate sensitive information within a decentralized database. According to Bhabendu Mohanta et al's (2019) review article and Enoch and Omijeh's (2023) supporting research article, they indicate a decentralized database has **multiple** points of failure. The benefits are reiterated here, as blockchain-decentralized databases do not require a third party management due to cryptographic algorithms **automating set processes and functions**, therefore making them immutable and trustworthy.

Wang et al. 's (2022) research article indicates that higher education institutions or even external organisations that focus on data security and transparency will favour decentralized databases. However, centralized databases may be chosen due to greater efficiency (performance and scalability). This argument is countered, as Qurotul Aini et al. 's (2022) research article indicates that **cryptographic solutions and strategies** may eliminate scalability issues. This is a recurring solution to a multitude of blockchain technology issues, as researchers have introduced their unique approaches to their specific organizations. This is clear with the examples of **'*CRL distribution points in conjunction with a Bloom filter*'**, **'*Blockcerts*'**, '"***hash-function Merkle tree*",** or **(IFPS).**

It is clear that Educational Resources (*Research Question 2*) **bleeds so heavily** from Security and Validity (*Research Question 1*), as there is prior-discussed evidence reiterating the points within this section. The only difference is contextual change from credential management to research management.

Significant Discourse within Collaboration and Expansion of Knowledge

Critical research findings include that blockchain technology, according to the authors within Gurung et al. 's (2023) research article, “Exploring Blockchain to Support Open Science Practices”, advocates for the concept of an ***‘Open Science’***. Blockchain technology may offer itself as an extremely valuable tool within educational resources, as the decentralized environment may provide **reliable** verification of data, **traceability** for educational resources, **appropriate accreditation** to the respective researchers, and peace of mind when information is shared - without the concern of security risk - and therefore encouraging collaborative efforts within research initiatives.

According to the World Economic Forum’s (2024) online article, “How universities can use blockchain to transform research”, The University of Utah had the privilege of participating as an ‘academic pioneer’ amongst National Science Data Fabric (**NSDF**) and National Data Platform (**NDP**). **N**ational **A**eronautics and **S**pace Administration (**NASA**) had been generous to allow access to multiple petabytes (in *Techtarget.com’s* online (2022) definition by Rodney Brown and Erin Sullivan, they indicate that a **petabyte** has approximately **1,024 terabytes**) of climate data. Due to blockchain technology’s ability to store an enormous amount of data without extreme local resources, therefore enhancing the quality of research, encouraging collaboration and broadening demographic perspectives.

However, according to Aghayev et al. 's (2008) research article, they had raised a particular concerning point where the sharing of private information in a centralized, standardized database that is accessible over the internet. Higher education institutions may feel **uncomfortable** releasing **valuable research**, **or** may want to **monetize** research to financially support the institution. This, therefore, brings up a discourse. While it was mentioned within a centralized, standardized database that is accessible over the internet, a decentralized blockchain database is an enhancement of that. Information would still be broadly available.

Moreover, in support of this, according to George Mensah’s (2023) research article, “Monetizing Research in the 21st Century: The Commercialization of Industrial and Social Sciences”, they highlight a critical point that monetizing research allows for the fostering of research collaborations, as well as enable future funding for further research and enhancements in **benefit** of the education institution. However, they also indicate that there may be an ethical concern around the restriction of research (Lemley et al., 2005), as they reference an additional article to support this statement. It

is extremely understandable of the monetary benefit of research monetization, as it may enable academic growth and sustainability especially within a higher education institution.

Therefore, the findings do not give a clear answer due to the above factors. **In unbiased conclusion**, it is ultimately up to an organisation or institution to how they would like to utilize blockchain technology within their educational resources, as both arguments offer a valid point to the discussion.

Conclusion

It is clear that this thesis has considered multiple elements in supporting the concept of applying blockchain technology to improve higher education. **The purpose** of the thesis is to indicate how security and validity may be used to combat identified and target problem areas, which is specifically fraud and counterfeiting credentials, and to indicate the cost of resources to maintain an innovative technology within the South African context. Additionally, the thesis aims to indicate how blockchain technology may be used to improve educational resources within the South African context. The research is aimed at filling a noticeable research gap in regards to assessing functionality and implementation within the boundaries of a South African higher education institution. A deductive research methodology had successfully been conducted and resulted in key findings with an appropriate amount of evidence to support the presented theories. Furthermore, the most important **key findings** indicate;

Credentialism had been an unexpected root socio-economic cause for counterfeiting and fraud, enticing the working class to lean towards illegal generation of academic credentials and qualifications in order to gain advantage with an (often found) unnecessarily overly competitive job market. However, this criminal activity is extremely unethical when credentials are extremely important within a specialised institution - especially the instance of hiring inadequate staff that may do harmful and/or severe damage within the institution and those who are affected. At this moment in time, results found that there is discourse on a theory of standardization. However, it is evident that blockchain technology is an extremely flexible and customizable tool that may be used to enhance systems within a higher education institution, including authenticating legitimate credentials and maintenance of educational resources. Conclusively, one shoe does not fit all. **In future work**, it is clear that it is up to the institution to identify its needs, its scale and its key problem areas in order to determine what algorithms, cryptographic techniques and affordance of resources they have to successfully implement and enhance their online learning experience and quality of life for staff, admin, students and external parties (in the context of outsiders authorizing credentials for future employees).

Blockchain technology that is implemented into a higher education system must be made aware that there are scalability and sustainability (energy consumption) issues in its bareboned infancy. Research had, therefore, suggested that there is a workaround to this in the form of various custom engineered frameworks that may be implemented and used to reduce cost of software and hardware

maintenance, and environmental fuels (electricity). Additionally, it was found to be difficult to recommend an appropriate, standardized blockchain system for higher education institutions due to the large variety of complex cryptographic techniques. Therefore**, in future work**, it is concluded that in order to offer a valid theory, quantitative research must be conducted before any system theorization and recommendation is put into place. It was found that all research papers had suggested blockchain-technology frameworks within an education system had an operating framework that was tested by surveyed users. Therefore, the thesis serves the **limitation** of not having an operating framework to conduct research on the exclusive needs in the context of the University of the Witwatersrand in South Africa. Additionally, the thesis indicated a **limitation** within its scope to be able to provide conclusive findings, as the methodology framework has indicated its **firm** approach on external research rather than experimental research. This is due to the limited scale of a Master's thesis, as well as a limitation of the researcher that had limited knowledge in practical algorithm engineering. However, the research presented gives insightful recommendations on which questions to ask and what actions must be taken **if the research is taken further in the future**.

In additional research **key findings**, steganography will still hold its place within a higher education institution as it merges with modern, innovative enhancements to institution biometrics, administrative processes and workflow of the student and lecturer. Additionally, this research proved itself vital due to the consideration of integrating physical documents into a digital database. Artificial intelligence may find its place within the implementation of blockchain technology, as it may prove valuable in assisting with a large workload when a merge may eventually occur. Converting old physical credentials, or transferring current databases to the new blockchain system may require a massive amount of labour. AI may assist with this. Despite what some researchers have theorized, further quantitative research found that training an institution (administrative staff, lecturers and students) to use a blockchain-based technology system will not be problematic if the design of the system is user friendly.

Actionable recommendations for institutions considering blockchain adoption, they may consider providing private keys for students within a reformed **DLT** (Distributed Ledger Technology). This ledger will use blockchain technology to verify credentials, as students will have their earned credentials hashed (placing their own digital fingerprint on them within the institution). The institution can then use **ECSDA** as an autonomous, 24/7 service for outsiders to verify credentials. The student may provide only their public key to whomever respectively requires to authenticate

their credentials, while their information is securely protected, **ECSDA** proves identity within the ledger as well as provides accurate information of transactions on the node (when the student graduates, their credentials are added as a block on the chain, filling a node and recording the input date. ECSDA will verify that the credential exists without disclosing sensitive information).

The possible positive **broader implications** of the research findings intertwine with the concept of **IOTs**, which are assistant technologies that connect to a network or cloud. Critical cybersecurity concerns were voiced by multiple researchers due to network and cloud vulnerabilities, and the research has indicated an explanation on how blockchain technology may have an extremely promising domino effect into external organizations and institutions that require additional security. In strong moral obligation, it has been firmly mentioned that blockchain technology demonstrated its potential to **save lives** through extremely impactful and tragic case studies. Blockchain technology may prevent **external** cybersecurity attacks, or even **internal** criminal activities due to the protective nature of automated and immutable security technologies.

Therefore, the **limitations** of the thesis proved that it could not answer proposed sub-research questions in Research Question 2 due to the need for dedicated and independent investigations into quantitative data. However, the **key findings** included a critical discourse if blockchain technology were to be implemented within educational resources such as collaborative accredited research databases. While blockchain technology and cryptographic techniques may be a sustainable and customizable tool to monitor academic conduct and enhance the quality of research, open-source databases may reduce the benefits of research monetization for higher education institutions. Ultimately, the **key findings** determine a stalemate between these two arguments, and have offered an unbiased recommendation that it is ultimately up to the higher education institution's generosity and availability of resources to decide if they were to introduce and utilize blockchain technology within a research database. Ultimately, a higher education institution may opt for a controlled, privatized, internal database **or** an international open-source collaborative database.

Therefore in **future work**, to reiterate, South African higher education institutions have great agency and customization when implementing blockchain-based technologies. Each institution has their own unique needs, applying specifically to the availability of their resources, scope and critical influence of their problems. It is within the bounds of the institution to conduct internal analysis of these aspects, and design blockchain-based systems on quantitative experimentation and findings. It

is worth consideration due to the evident ability to improve the quality and integrity of internal and external operations and functions within the institution's ecosystem.

References

1. *About mie* (2023) *Managed Integrity Evaluation (MIE) Background Screening*. Available at: https://www.mie.co.za/background-screening/index-2015/about-mie (Accessed: 28 June 2023).
2. Aghayev, E. *et al.* (2008) 'Virtopsy – the concept of a centralized database in forensic medicine for analysis and comparison of radiological and autopsy data', *Journal of Forensic and Legal Medicine*, 15(3), pp. 135–140. doi:10.1016/j.jflm.2007.07.005.
3. Aini, Q. *et al.* (2022) 'Blockchain based Certificate Verification System Management,' *Aptisi Transactions on Management* (ATM), 7(3), pp. 1–10. https://doi.org/10.33050/atm.v7i3.1922.
4. Akinradewo, O.I. *et al.* (2022) 'A principal component analysis of barriers to the implementation of blockchain technology in the South African Built Environment', *Journal of Engineering, Design and Technology*, 20(4), pp. 914–934. doi:10.1108/jedt-05-2021-0292.
5. Alammary, A. *et al.* (2019) 'Blockchain-based applications in education: A systematic review', *Applied Sciences*, 9(12), p. 2400. doi:10.3390/app9122400.
6. Albeanu, G. (2017) 'Blockchain technology and education', *In The 12th International Conference on Virtual Learning ICVL*, pp. 271-275. https://bit.ly/3MqIXTj
7. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric Encryption Algorithms: Review and Evaluation study. In *Article in International Journal of Communication Networks and Information Security* (Vol. 12, Issue 2). https://www.researchgate.net/publication/349324592
8. AlKhanafseh, M. and Surakhi, O. (2024) *A new evidence preservation forensics model using blockchain and stenography techniques* [Preprint]. doi:10.20944/preprints202403.0703.v1.
9. Aumasson, J.-P. (2024) *Serious Cryptography, 2nd Edition: A Practical Introduction to Modern Encryption*. NO STARCH PRESS, INC.
10. Alshambri, H.A. and Alassery, F. (2021) 'Securing Fog computing for E-Learning system using integration of two encryption algorithms,' *Journal of Cyber Security*, 3(3), pp. 149–166. https://doi.org/10.32604/jcs.2021.022112.
11. 'artificial intelligence' (2025). https://dictionary.cambridge.org/dictionary/english/artificial-intelligence.

12. Awaji, B. and Solaiman, E. (2022) *Design, implementation, and evaluation of Blockchain-Based Trusted Achievement Record System for students in Higher Education*. https://arxiv.org/abs/2204.12547?
13. Balobaid, A.S. *et al.* (2023) 'Modeling of blockchain with encryption based secure education record management system,' *Egyptian Informatics Journal*, 24(4), p. 100411. https://doi.org/10.1016/j.eij.2023.100411.
14. Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the Efficiency and Reliability of Digital Time-Stamping. In R. Capocelli, A. De Santis, & U. Vaccaro (Eds.), *Sequences* II (pp. 329-334). New York, NY *Springer*.
15. Bevers, J. (2021) *The Study of Symmetric and Asymmetric Key Encryptions*. Doctoral dissertation. University Honors College, Middle Tennessee State University.
16. Bi, W., Jia, X. and Zheng, M. (2018) *A secure multiple elliptic curves digital signature algorithm for blockchain*. https://arxiv.org/abs/1808.02988.
17. Black, J. and Fullerton, C. (2020) 'Digital Deceit: fake news, artificial intelligence, and censorship in educational research,' *Open Journal of Social Sciences*, 08(07), pp. 71–88. https://doi.org/10.4236/jss.2020.87007.
18. Brown, R. and Sullivan, E. (2022) *petabyte*. https://www.techtarget.com/searchstorage/definition/petabyte.
19. Chadwick, D.W., Tassabehji, R. and Young, A. (2000) 'Experiences of using a public key infrastructure for the preparation of examination papers,' *Computers & Education*, 35(1), pp. 1–20. https://doi.org/10.1016/s0360-1315(99)00040-8.
20. Chen, G. *et al.* (2018) 'Exploring blockchain technology and its potential applications for Education', *Smart Learning Environments*, 5(1). doi:10.1186/s40561-017-0050-x.
21. Chen, G. (2024) 'Optimizing digital signatures for enhanced privacy protection in blockchain systems,' *Applied and Computational Engineering*, 110(1), pp. 96–101. https://doi.org/10.54254/2755-2721/110/2024melb0105.
22. Computer Security Division, I.T.L. (2023) *Hash functions*: CSRC, CSRC. Available at: https://csrc.nist.gov/projects/hash-functions#:~:text=Approved%20Algorithms,-A%20hash%20algorithm&text=FIPS%20180%2D4%20specifies%20seven,and%20SHA%2D512%2F256. (Accessed: 18 July 2023).
23. Creswell, J.W. and Creswell, J.D. (2017) *Research design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.
24. *Cross-disciplinary definition & meaning* (2024) *Dictionary.com*. Available at: https://www.dictionary.com/browse/cross-disciplinary (Accessed: 09 December 2024).

25. Crowe, S. *et al.* (2011) 'The case study approach', *BMC Medical Research Methodology*, 11(1). doi:10.1186/1471-2288-11-100.
26. *Degree verification* (2025). https://ucentralasia.org/schools/registrar/degree-verification.
27. Department of Health (2019) *National Digital Health Strategy for South Africa 2019-2024*, *World Health Organization*. Available at: https://extranet.who.int/mindbank/item/7358#:~:text=The%20National%20Digital%20Health%20Strategy,conjunction%20with%20other%20government%20departments. (Accessed: 05 November 2024).
28. Developer (2023) *Credentials on Blockchain - City University of Paris*. https://cityuparis.fr/credentials-on-blockchain/.
29. Dhawan, S. (2020) 'Online learning: a panacea in the time of COVID-19 crisis,' *Journal of Educational Technology Systems*, 49(1), pp. 5–22. https://doi.org/10.1177/0047239520934018.
30. *Digital Diploma debuts at MIT* (2017). https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017.
31. emn178 (2025) *SHA512/256*, *Online Tools*. Available at: https://emn178.github.io/online-tools/sha512_256.html (Accessed: 29 January 2025).
32. Enoch, J. D., Omijeh, B. O. and Okeke, R. O. (2023) "Comparative Analysis of Blockchain and Database", *European Journal of Science, Innovation and Technology*, 3(3), pp. 454-463. Available at: https://ejsit-journal.com/index.php/ejsit/article/view/233 (Accessed: 19 February 2025).
33. 'Fenny: Word of the day' (2025) *Dictionary.com*. https://www.dictionary.com/browse/counterfeit.
34. Gauravaram, P. (2007) *Cryptographic Hash Functions: Cryptanalysis, Design and Applications*. Doctoral dissertation. Queensland University of Technology.
35. GeeksforGeeks (2022) *Blockchain hash function*, *GeeksforGeeks*. Available at: https://www.geeksforgeeks.org/blockchain-hash-function/ (Accessed: 17 December 2024).
36. George, L. and J. Kizhakkethottam, J. (2021) 'A comparative study of zero knowledge proof and homomorphic encryption in guaranteeing data privacy in Blockchain Applications', *International Journal of Advanced Research*, 9(02), pp. 359–361. doi:10.21474/ijar01/12455.
37. Guernsey, L. (1997) 'Is the Internet Becoming a Bonanza for Diploma Mills?', *Chronicle of Higher Education*, 44(17).

38. Habbal, F. (2023) 'The implications and efficacy of online verification tools in scientific research and citation practices,' *International Journal of Automation and Digital Transformation*, 2(1), pp. 4–14. https://doi.org/10.54878/mnart786.
39. *Hash-function definition* (2024) *YourDictionary*. Available at: https://www.yourdictionary.com/hash-function (Accessed: 18 December 2024).
40. Haque, Md.M. *et al.* (2020) 'An innovative approach of verification mechanism for both electronic and printed documents', *International Journal of Advanced Computer Science and Applications*, 11(8). doi:10.14569/ijacsa.2020.0110876.
41. Hoseini, S.V. (2018) 'Mathematics and data structures in blockchain and Ethereum,' *ResearchGate* [Preprint]. https://doi.org/10.13140/RG.2.2.35846.52805/1.
42. Islam, S. and Apu, K.U. (2024) 'DECENTRALIZED VS. CENTRALIZED DATABASE SOLUTIONS IN BLOCKCHAIN: ADVANTAGES, CHALLENGES, AND USE CASES,' *Global Mainstream Journal of Innovation, Engineering & Emerging Technology.*, 3(4), pp. 58–68. https://doi.org/10.62304/jieet.v3i04.195.
43. Jayabalasamy, G. and Koppu, S. (2022) 'An empirical study to demonstrate that EDDSA can be used as a performance improvement alternative to ECDSA in Blockchain and IOT', *Informatica*, 46(2). doi:10.31449/inf.v46i2.3807.
44. Jimu, I.M. (2018) *Fake qualifications and the challenge of regulating higher education in ...* Available at: https://pdfs.semanticscholar.org/bf79/3375b2fe7aaad139e66322fb6383b22c08c5.pdf (Accessed: 19 June 2023).
45. Katz, J. and Lindell, Y. (2007) *Introduction to modern cryptography: principles and protocols*. Chapman and Hall/CRC.
46. Kaufmann, A. and Gartmon, E. (2024) *Comparative analysis of different cryptographic hash functions*. https://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A1885074&dswid=-4906.
47. Kaushik, R. and Thakur, A. (2022) 'A Brief Review on IoT, its Applications, Challenges & Future Aspects in Aviation Industry,' *ResearchGate* [Preprint]. https://www.researchgate.net/publication/361457548_A_Brief_Review_on_IoT_its_Applications_Challenges_Future_Aspects_in_Aviation_Industry.
48. Kelly, L.M. and Cordeiro, M. (2020) 'Three principles of pragmatism for research on Organizational Processes', *Methodological Innovations*, 13(2), p. 205979912093724. doi:10.1177/2059799120937242.

49. Kim, S.-K. (2022) 'Blockchain Smart contract to prevent forgery of degree Certificates: Artificial Intelligence Consensus Algorithm,' *Electronics*, 11(14), p. 2112. https://doi.org/10.3390/electronics11142112.
50. Kim, S. and Kim, D. (2024) 'Data-Tracking in Blockchain Utilizing Hash Chain: A study of Structured and Adaptive process,' *Symmetry*, 16(1), p. 62. https://doi.org/10.3390/sym16010062.
51. King, C. (2022) 'Some mathematical topics in blockchain and digital ledger technology'
52. King, J.L. (1983) 'Centralized versus decentralized computing: organizational considerations and management options', *ACM Computing Surveys*, 15(4), pp. 319–349. doi:10.1145/289.290.
53. Krzyzanowski, P. (2024) *Steganography &watermarking*. Available at: https://people.cs.rutgers.edu/~pxk/419/notes/steganography.html (Accessed: 11 November 2024).
54. Kuznetsov, A. *et al.* (2021) 'Performance analysis of cryptographic hash functions suitable for use in blockchain', *International Journal of Computer Network and Information Security*, 13(2), pp. 1–15. doi:10.5815/ijcnis.2021.02.01.
55. Ledwaba, K. (2018) 'Unizulu professor killed over fraudulent PhDs,' *SowetanLIVE*, 3 December. https://www.sowetanlive.co.za/news/south-africa/2018-12-03-unizulu-professor-killed-over-fraudulent-phds/#google_vignette.
56. Leibson, S. (2018) *Blockchain is not Bitcoin—Bitcoin is not Blockchain*, *eejournal*. Available at: https://www.eejournal.com/article/blockchain-is-not-bitcoin-bitcoin-is-not-blockchain/ (Accessed: 28 August 2023).
57. Lemley, M.A. (2011) 'Are universities patent trolls?,' in *Cambridge University Press eBooks*, pp. 531–546. https://doi.org/10.1017/cbo9781139051262.021.
58. Li, R. (2022) *South Africa regulates crypto: Alb Article*, *ALB Legal and Business Issues from Africa*. Available at: https://www.africanlawbusiness.com/news/18291-south-africa-regulates-crypto (Accessed: 19 June 2023).
59. Look, M. (2011) *How to add a watermark to photos*, *HowStuffWorks*. Available at: https://electronics.howstuffworks.com/cameras-photography/tips/how-to-place-watermarks-on-pictures.htm (Accessed: 24 June 2024).
60. Lucas, E. (2019a) *The spycraft revolution*, *Foreign Policy*. Available at: https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/ (Accessed: 09 July 2024).

61. Mathe, R., Atukuri, V. and Devireddy, S.K. (2012) 'Securing information: cryptography and steganography', *International Journal of Computer Science and Information Technologies*, 3(3), pp.4251-4255.
62. Matlebjane, D.A. and Ndayizigamiye, P. (2022) 'Antecedents of the adoption of blockchain to enhance patients' health information management in South Africa', *SA Journal of Information Management*, 24(1). doi:10.4102/sajim.v24i1.1552.
63. Maxwell, J.A. (2023) *Qualitative research design an interactive approach*. 3rd edn. Thousand Oaks: SAGE Publications.
64. McDermid, D. (no date) *Pragmatism*, *Internet encyclopedia of philosophy*. Available at: https://iep.utm.edu/pragmati/#:~:text=Pragmatism%20is%20a%20philosophical%20movement,ideas%20are%20to%20be%20rejected. (Accessed: 30 November 2023).
65. MDV Edwards (2022) *Leaning coconuts and well maintained grass lawn fronting the beach. At a luxury resort in Dumaluan Beach, Panglao Island, Bohol, Philippines.*, *Shuttershock*. Available at: https://www.shutterstock.com/image-photo/leaning-coconuts-well-maintained-grass-lawn-2221498083 (Accessed: 24 June 2024).
66. Melnikovas, A. (2018) 'Towards an explicit research methodology: adapting research onion model for futures studies,' *Journal of Futures Studies*, 23(2), pp. 29–44. https://doi.org/10.6531/jfs.201812_23(2).0003.
67. Mensah, G.B. (2023) 'Monetizing research in the 21st century: the commercialization of industrial and social sciences,' *ResearchGate* [Preprint]. https://doi.org/10.13140/RG.2.2.36809.52328.
68. Mohammed, A. and Saleh, B.M. (2017) 'Centralized database: A prerequisite for security and sustainable development in Nigeria', *International Journal of Innovative Research in Computer Science & Technology*, 5(1), pp. 209–213. doi:10.21276/ijircst.2017.5.1.7.
69. Mohanta, B.K. *et al.* (2019) 'Blockchain technology: A survey on applications and security privacy Challenges,' *Internet of Things*, 8, p. 100107. https://doi.org/10.1016/j.iot.2019.100107.
70. Mwandosya, M.J. and Luhanga, M.L. (2020) *Blockchain: a disruptive and transformative technology of the Fourth Industrial Revolution*. https://journals.udsm.ac.tz/index.php/bmr/article/view/3900.
71. National Department of Health (2019) *National Digital Health Strategy for South Africa*. Available at: https://health.gov.za/wp-content/uploads/2020/11/national-digital-strategy-for-south-africa-2019-2024-b.pdf (Accessed: 21 July 2023).

72. Ndlovu, L. and Leslie, A.B. (2022) 'False or fake qualifications in an employment context: a South African perspective,' *ResearchGate* [Preprint]. https://doi.org/10.20473/ydk.v37i3.367.
73. Pandya, M. (2024) 'Performance evaluation of hashing algorithms on commodity hardware,' *arXiv (Cornell University)* [Preprint]. https://doi.org/10.48550/arxiv.2407.08284.
74. Paradis, E. *et al.* (2016) 'Design: Selection of data collection methods', *Journal of Graduate Medical Education*, 8(2), pp. 263–264. doi:10.4300/jgme-d-16-00098.1.
75. *Pedagogy definition & meaning* (2024) *Dictionary.com*. Available at: https://www.dictionary.com/browse/pedagogy (Accessed: 23 October 2024).
76. Pu, S. and Lam, J.S.L. (2022) 'The benefits of blockchain for digital certificates: A multiple case study analysis,' *Technology in Society*, 72, p. 102176. https://doi.org/10.1016/j.techsoc.2022.102176.
77. *Quantum Computer Definition & meaning* (2025) *Dictionary.com*. Available at: https://www.dictionary.com/browse/quantum-computer (Accessed: 18 February 2025).
78. Rahman, T. *et al.* (2023) 'Verifi-Chain: a credentials verifier using blockchain and IPFS,' in *Lecture notes in networks and systems*, pp. 361–371. https://doi.org/10.1007/978-981-99-5166-6_24.
79. Rana, D. (2024) 'Advancements and comparative analysis of Digital Signature Algorithms: A Review', *International Journal for Research in Applied Science and Engineering Technology*, 12(5), pp. 5778–5792. doi:10.22214/ijraset.2024.62955.
80. Saunders, M., Lewis, P. & Thornhill, A. (2003), *Research methods for business students*, Pearson education limited, England.
81. Semilof, M. and Clark, C. (2023) *What is steganography?: Definition from TechTarget*, *Security*. Available at: https://www.techtarget.com/searchsecurity/definition/steganography (Accessed: 24 June 2024).
82. Sharma, S. and Mishra, M. (2024) *(PDF) Cryptographic Hash Functions: A Review*, *ResearchGate*. Available at: https://www.researchgate.net/publication/267422045_Cryptographic_Hash_Functions_A_Review (Accessed: 06 January 2025).
83. Sheldon, R. (2021) *A timeline and history of Blockchain technology*, *WhatIs.com*. Available at: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology (Accessed: 19 June 2023).
84. Sobti, R. and Ganesan, G. (2012) 'Cryptographic Hash Functions: A review,' *ResearchGate* [Preprint].

https://www.researchgate.net/publication/267422045_Cryptographic_Hash_Functions_A_Review.

85. Springer, J. and Haindl, P. (2024) 'Blockchain-based PKI within a Corporate Organization: Advantages and Challenges,' *arXiv (Cornell University)* [Preprint]. https://doi.org/10.48550/arxiv.2407.04536.
86. *Spycraft definition* (2024) *YourDictionary*. Available at: https://www.yourdictionary.com/spycraft (Accessed: 01 July 2024).
87. Statistic South Africa. (2016). Quarterly Labour Force Survey (QLFS), 4th Quarter 2016, released February 2017
88. Tahir, R. (2018) 'A study on malware and malware detection techniques', *International Journal of Education and Management Engineering*, 8(2), pp. 20–30. doi:10.5815/ijeme.2018.02.03.
89. Tariq, A., Haq, H.B. and Ali, S.T. (2019) 'Cerberus: a Blockchain-Based accreditation and degree verification system,' *arXiv (Cornell University)* [Preprint]. https://doi.org/10.48550/arxiv.1912.06812.
90. Tshifura, L. (2022) 'UJ implements Blockchain-based Certificates for graduates,' *University of Johannesburg News*, 19 April. https://news.uj.ac.za/news/uj-implements-blockchain-based-certificates-for-graduates-2-2/.
91. Turkanović, M. *et al.* (2017) 'EduCTX: A blockchain-based higher education credit platform,' *ResearchGate* [Preprint]. https://doi.org/10.48550/arXiv.1710.09918.
92. *University of Melbourne to issue recipient-owned blockchain records* (2017). https://www.unimelb.edu.au/newsroom/news/2017/october/university-of-melbourne-to-issue-recipient-owned-blockchain-records.
93. Usman, M. (2022) 'Understanding cryptocurrency, blockchain and the market,' *ResearchGate* [Preprint]. https://www.researchgate.net/publication/373143335_Understanding_Cryptocurrency_Blockchain_and_the_Market#pf30.
94. Vaismoradi, M., Turunen, H. and Bondas, T. (2013) 'Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study', *Nursing & Health Sciences*, 15(3), pp. 398–405. doi:10.1111/nhs.12048.
95. Wang, H., Xu, C., Zhang, C., Xu, J., Peng, Z. and Pei, J. (2022) 'vChain+: Optimizing Verifiable Blockchain Boolean Range Queries', *2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia*, pp. 1927–1940. doi: 10.1109/ICDE53745.2022.00190.

96. *What is a symmetric key*? (2024) *Thales*. Available at: https://cpl.thalesgroup.com/faq/key-secrets-management/what-symmetric-key#:~:text=In%20cryptography%2C%20a%20symmetric%20key,was%20used%20to%20encrypt%20it. (Accessed: 19 August 2024).
97. Woiceshyn, J. and Daellenbach, U. (2018) 'Evaluating inductive vs Deductive Research in Management Studies', *Qualitative Research in Organizations and Management: An International Journal*, 13(2), pp. 183–195. doi:10.1108/qrom-06-2017-1538.
98. Yakubov, A. *et al.* (2018) 'A blockchain-based PKI management framework,' *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–6. https://doi.org/10.1109/noms.2018.8406325.
99. Yasar, K. and Gillis, A.S. (2024) *internet of things (IoT)*. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT.
100. Yli-Huumo, J. *et al.* (2016) 'Where is current research on blockchain Technology?—A systematic review,' *PLoS ONE*, 11(10), p. e0163477. https://doi.org/10.1371/journal.pone.0163477.
101. Young, S.D. (2023) *OpenZeppelin reveals top 10 blockchain hacking techniques in 2022*, *CoinDesk Latest Headlines* RSS. Available at: https://www.coindesk.com/tech/2023/03/17/open-zeppelin-reveals-top-10-blockchain-hacking-techniques-in-2022/ (Accessed: 26 June 2023).

All infographics, charts and diagrams have been made with the assistance of LucidChart's free diagramming software. URL: https://www.lucidchart.com/pages/